SuperStack® 3
Server Load Balancer
Server Load Balancer Plus
User Guide

3C16120
3C16121

http://www.3com.com/

Part No. 990-0049-00
Published June 2001

3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

CONTENTS

About This Guide

This guide provides all the information you need to install and use a SuperStack® 3 Server Load Balancer (3C16120) or the SuperStack 3 Server Load Balancer Plus (3C16121) to perform server load balancing, both non-redundant and redundant, and cache redirection.

The guide is intended for use by network administrators who are responsible for installing and setting up network equipment.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com® World Wide Web site:

http://www.3com.com/

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

Table 2 Text Conventions

Convention	Description
`boldface`	This typeface represents user input. Example: At the login: prompt, enter **`admin`**.
`Screen displays`	This typeface represents information as it appears on the screen.
`Syntax`	The word "syntax" means that you must evaluate the syntax provided and then supply the appropriate values for the placeholders that appear in angle brackets. Example: To change your password, use the following syntax: `system password <password>` In this example, you must supply a password for <password>.
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.

Related Documentation

In addition to this guide, the documentation set includes the following:

- *Release Notes (PDF format)*

  These notes provide information about the current software release, including new features, modifications, and known problems. These release notes are available in PDF format and are accessible from the 3Com web site.

There are other publications you may find useful, such as:

- Documentation accompanying the Advanced Redundant Power System.
- Documentation accompanying the 3Com® Network Supervisor.

Product Registration

You can register your SuperStack 3 Server Load Balancer on the 3Com Web site to receive up-to-date information on your product:

`http://support.3com.com/registration/frontpg.pl`

Documentation Comments

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

pddtechpubs_comments@3com.com

Please include the following information when commenting:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- SuperStack 3 Server Load Balancer and Server Load Balancer Plus User Guide
- Part Number 990-XXXX-XX
- Page 21

1 INTRODUCING THE SERVER LOAD BALANCER

This chapter contains introductory information about the SuperStack® 3 Server Load Balancer and the SuperStack 3 Server Load Balancer Plus. It covers summaries of the following topics:

- About the Server Load Balancer
- Server Load Balancer — Front View Detail
- Server Load Balancer — Rear View Detail
- Downloading 3Com Network Supervisor

Unless otherwise noted, the information in this chapter applies to both the Server Load Balancer and the Server Load Balancer Plus.

About the Server Load Balancer

The SuperStack® 3 Server Load Balancer and Server Load Balancer Plus provide support for connecting multiple high-performance servers to a Gigabit backbone and providing server load balancing, cache redirection and security functionality.

Summary of Hardware Features

Table 3 summarizes the hardware features that are supported in both models of the Server Load Balancer.

Table 3 Hardware Features

Feature	Server Load Balancer Server Load Balancer Plus
Memory	■ 64 MB for Server Load Balancer Plus ■ 32 MB for Server Load Balancer
12 10/100 LAN Ports	Supported
2 Gigabit Ethernet Ports	Supported
SuperStack 3 Architecture	■ Connects to a SuperStack 3 Advanced Redundant Power System (ARPS) ■ Installs in a 19-inch rack or stand-alone mounting

Summary of Software Features

Table 4 summarizes the software features that are supported in both models of the Server Load Balancer.

Table 4 Software Features

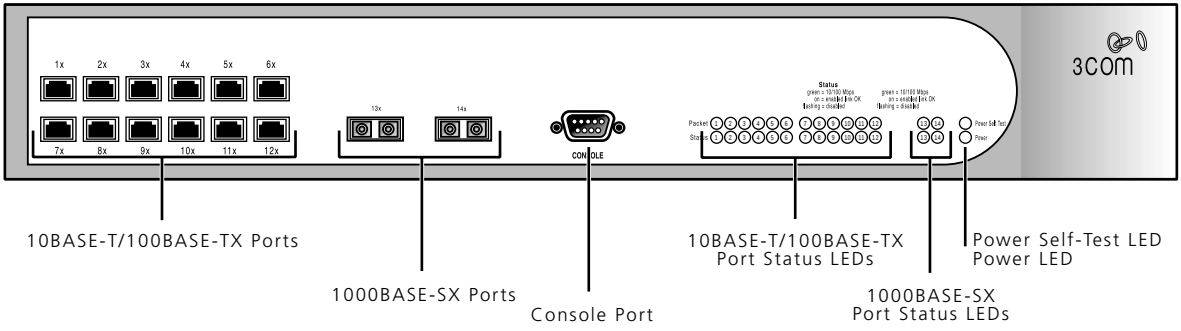
Feature	Server Load Balancer Server Load Balancer Plus
Algorithms	■ Round Robin ■ Weighted Round Robin ■ Least Connections ■ Quickest Last Response ■ Quickest Average Response ■ Weighted Percentage
Port Trunking (Etherchannel)	Supported
Up to 256 servers	Supported
TCP/IP Sessions	■ 16,000 for the Server Load Balancer ■ 128,000 for the Server Load Balancer Plus
Persistence Modes	■ Source IP ■ Secure Socket Layer (SSL) Session ID ■ Cookie

Table 4 Software Features

Feature	Server Load Balancer Server Load Balancer Plus
Cache Redirection	■ Transparent mode ■ Proxy mode
DoS Protection	Supported
Redundant Failover Modes	■ Primary/Secondary ■ Active/Active
Management	Web interface, command line interface, and SNMP supported

Server Load Balancer — Front View Detail

Figure 1 Server Load Balancer — front view



Ports The Server Load Balancer and Server Load Balancer Plus have twelve dedicated 10BASE-T/100BASE-TX ports and two 1000BASE-SX ports.

Console Port The console port allows you to use a terminal or serial PC connector to access the command line interface (CLI). The CLI allows you to assign the IP address to the Service Load Balancer and provides basic configuration capabilities. For console port pin-out information, see Appendix B.

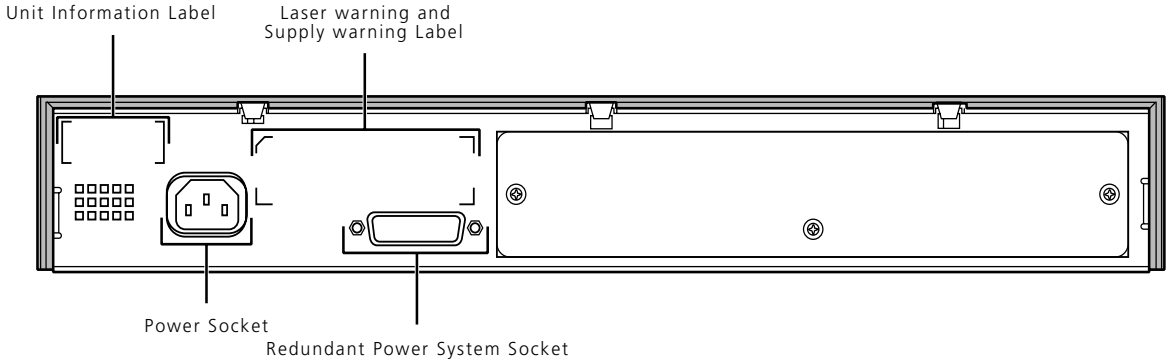
LEDs Table 5 lists LEDs visible on the front of the Server Load Balancer, and how to read their status according to color.

Table 5 LED Behavior

LED	Color	Indicates
Power/Self Test LED		
	Yellow	The Server Load Balancer has failed its Power On Self Test (POST) or a failure is detected in the runtime.
	Yellow flashing	The Server Load Balancer is running POST.
	Off	No fault has been detected.
Power LED		
	Green	The Server Load Balancer is receiving power.
	Green flashing	The Server Load Balancer is receiving power and downloading new operating software.
	Off	The Server Load Balancer is not receiving power.
10/100BASE-T Port Status LEDs		
Packet	Yellow	Packets are being transmitted/received on the port.
	Off	No packets are being transmitted/received on the port.
Status	Green	A link is present and the port is enabled.
	Green flashing	The port is disabled.
	Off	No link is present.
1000BASE-SX Port Status LEDs		
Packet	Yellow	Packets are being transmitted/received on the port.
	Off	No packets are being transmitted/received on the port.
Status	Green	A high speed (1000 Mbps) link is present, and the port is enabled.
	Green flashing	A high speed (1000 Mbps) port is disabled.
	Off	No link is present.

Server Load Balancer — Rear View Detail

Figure 2 Server Load Balancer — rear view



Unit Information Label

The labels on the rear of the unit show the following:

- The 3Com product name of the Server Load Balancer
- The 3Com 3C number of the Server Load Balancer
- The unique MAC address (Ethernet address) of the Server Load Balancer
- The serial number of the Server Load Balancer

You may need this information for fault reporting purposes.

Power Socket

The Server Load Balancer automatically adjusts its power setting to any supply voltage in the range 90-240 VAC.

Advanced Redundant Power System Socket

To protect against internal power supply failure, you can use this socket to connect a Advanced Redundant Power System (ARPS) (part number 3C16075) to the Server Load Balancer. For more information on the Advanced Redundant Power System, see the documentation shipped with the power system.

For normal redundancy, the unit requires one Type 3 Power Module (part number 3C16075).

For full redundancy, the unit requires two Type 3 Power Modules combined using a Type 3 Y-Cable (part number 3C16077).

CAUTION: *The Server Load Balancer can only use a SuperStack Advanced Redundant Power System output.*

WARNING: *If you are connecting the Server Load Balancer to a ARPS Type 3 Power Module, read the Safety Information section in the documentation shipped with the power system.*

CAUTION: *The Server Load Balancer has no ON/OFF switch; the only method of connecting or disconnecting main power is by connecting or disconnecting the power cord.*

Downloading 3Com Network Supervisor

You can download 3Com Network Supervisor Version 3.0 from the following Web address:

`http://www.3com.com/tns`

Network Supervisor is a powerful, intuitive network management application for small to medium enterprise networks.

Network Supervisor automatically discovers up to 1500 network devices and shows devices and connections on a graphical display. Network managers can view network activity, monitor stress and set thresholds and alerts. This information helps to provide the most efficient, cost-effective use of network resources.

Version 3.0 adds significant extra functionality designed to detect network inefficiency and optimize network performance. Features include support for related and recurring events, user definable reports, auto-alerting using pager or SMS messages and simple updates from the 3Com Web site.

3Com Network Supervisor offers Telnet and Web device management.

2 Installing the Server Load Balancer

This chapter contains the information you need to install and set up the Server Load Balancer. It covers the following topics:

- Package Contents
- Choosing a Suitable Site
- Rack-mounting
- Placing Units On Top of Each Other
- The Power-up Sequence
- Solving Problems Indicated by LEDs

WARNING: Safety Information. *Before installing or removing any components from the Server Load Balancer or carrying out any maintenance procedures, you must read the safety information provided in Appendix A of this guide.*

AVERTISSEMENT: Consignes de sécurité. *Avant d'installer ou d'enlever tout composant du Server Load Balancer ou d'entamer une procédure de maintenance, lisez les informations relatives à la sécurité qui se trouvent dans l'Appendice A de ce guide.*

WARNHINWEIS: Sicherheitsinformationen. *Bevor Sie Komponenten aus dem Server Load Balancer entfernen oder dem Server Load Balancer hinzufuegen oder Instandhaltungsarbeiten verrichten, lesen Sie die Sicherheitsanweisungen, die in Appendix A (Anhang A) in diesem Handbuch aufgefuehrt sind.*

Package Contents

Your shipping container should contain the following items:

- Server Load Balancer (3C11620)
  or Server Load Balancer Plus (3C11621)
- User Guide (this guide)
- Power Cord
- 2 x mounting brackets
- 6 x screws
- 4 x rubber feet

Choosing a Suitable Site

The Server Load Balancer is suited for use where it can be mounted in a standard 19-inch equipment rack, or free-standing. A rack-mounting kit, containing two mounting brackets and six screws is supplied with the unit.

CAUTION: *Ensure that the ventilation holes are not obstructed.*

When deciding where to position the Server Load Balancer, ensure that:

- Cabling is located away from sources of electrical noise such as radios, transmitters and broadband amplifiers.
- Cabling is located away from power lines and fluorescent lighting fixtures
- The Server Load Balancer is accessible and cables can be connected easily.
- Water or moisture cannot enter the case of the Server Load Balancer.
- Air-flow is not restricted around the Server Load Balancer or through the vents in the side of the Server Load Balancer. 3Com recommends that you provide a minimum of 25 mm (1 in.) clearance.
- The air is as free from dust as possible.
- No more than four Server Load Balancer units are placed on top of one another, if the units are free-standing.
- Temperature operating limits are not exceeded. It is recommended that the unit is installed in a clean, air conditioned environment.
- Ensure there is adequate clearance at the front of the unit to ensure that the fibers are not damaged as they have a restricted bend radius.

Rack-mounting

The Server Load Balancer is 1.5U and fits in most standard 19-inch racks. However, if you are connecting the Server Load Balancer to a ARPS Type 3 power module, a runner, shelf or tray is recommended to support the additional weight. You will need to allow a 2U space within the rack for each Server Load Balancer.

WARNING: *The rack-mount kits alone are not sufficient to support the weight of the Server Load Balancer when attached to an ARPS power module. It is recommended that you use a runner, shelf or tray to support the total weight. The rack mount kits must not be used to suspend the Server Load Balancer from under a table or desk, or attach it to a wall.*

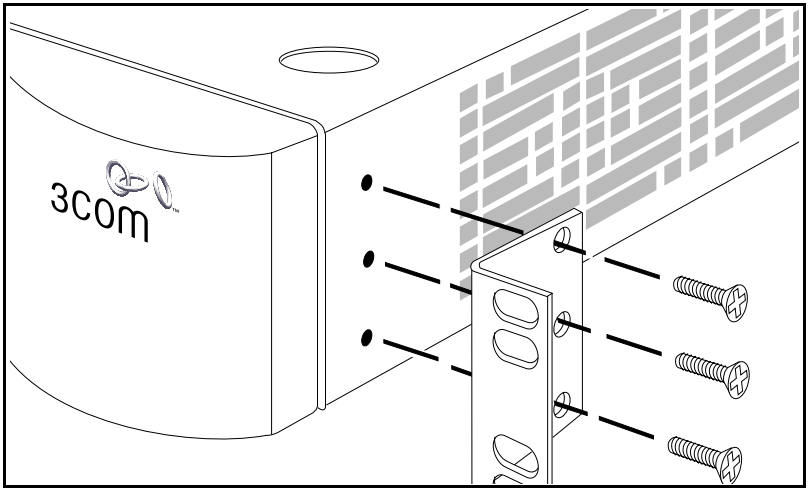
CAUTION: *You must use a full depth shelf or support that will not obstruct the air flow through the side panels of the Server Load Balancer.*

CAUTION: *Disconnect all cables from the Server Load Balancer before continuing. Remove all self adhesive pads from the underside of the Server Load Balancer if they have been fitted.*

To rack-mount your Server Load Balancer:

1. Place the unit the right way up on a hard flat surface, with the front facing towards you.
2. Locate a mounting bracket over the mounting holes on one side of the unit, as shown in Figure 3.

Figure 3 Fitting a bracket for rack-mounting



You must use the screws supplied with the mounting brackets. Damage caused to the unit by using incorrect screws invalidates your warranty.

3 Insert the three screws and tighten with a suitable screwdriver.

4 Repeat steps 2 and 3 for the other side of the unit.

5 Insert the unit into the 19-inch rack and secure with suitable screws (not provided). Ensure that ventilation holes are not obstructed.

6 Connect network cabling.

Choosing the Correct Cables

The 1000BASE-FX fiber optic LAN ports (Ports 13 and 14) on the Server Load Balancer use SC connectors. The 10BASE-T/100BASE-TX copper LAN ports (Ports 1 through 12) use RJ45 connectors.

Table 6 explains cables to use before connecting a device to the copper ports.

Table 6 Cabling for Copper Ports

Device to Connect:	Use this Cable:
Another Server Load Balancer, a network switch or router	Crossover cable[1]
End Station (such as a server or a PC)	Straight-through cable[1]

[1] Cables are not supplied by 3Com.

Placing Units On Top of Each Other

If the units are free-standing, up to four units can be placed one on top of the other.

If you are placing units one on top of the other, you must use the self-adhesive rubber feet supplied. Apply the feet to the underside of each unit, sticking one in the marked area at each corner. Place the units on top of each other, ensuring that the feet of the upper unit line up with the recesses of the lower unit.

The Power-up Sequence

The following sections describe how to get your Server Load Balancer powered-up and ready for operation.

WARNING: *If you are connecting the Server Load Balancer to a ARPS Type 3 Power Module, read the Safety Information section in the documentation shipped with the power system.*

Powering-up

To power-up the Server Load Balancer, complete the following steps:

1. Plug the power cord into the power socket at the rear of the unit.
2. Plug the other end of the power cord into your power outlet.

   The unit powers-up and runs through its Power On Self Test (POST), which takes approximately 10 seconds.

   During the POST, all ports on the Server Load Balancer are disabled and the LEDs light in a rapid sequence. See "LEDs" on page 14.

   When the POST has completed, check the Power/Self Test LED to make sure that your Server Load Balancer is operating correctly. See "Solving Problems Indicated by LEDs" on page 22.

Solving Problems Indicated by LEDs

Table 7 contains a list of problems and suggested solutions if the LEDs indicate a problem. For Technical Support information, see Appendix C.

Table 7 Problems Indicated by LEDs

Problem	Suggested Solution
The Power LED does not light	Check that the power cable is firmly connected to the relevant unit and to the supply outlet. If the connection is secure and there is still no power, you may have a faulty power cord.
On powering-up, the Power/Self Test LED lights yellow	The relevant unit has failed its Power On Self Test (POST) because of an internal problem. Contact your supplier for advice.
A link is connected and yet the Status LED for the port does not light	Check that: ■ All connections are secure. ■ The devices at both ends of the link are powered-up. ■ The devices at both ends of the link have the same auto-negotiation setting, i.e. both enabled, or both disabled. ■ The quality of cable is satisfactory. ■ The correct type of cable (crossover or straight-through) is used.

3 Setting Up for Management

This chapter explains the management methods used for managing a Server Load Balancer, and details the steps required before you can configure a Server Load Balancer to suit the needs of your network. It covers the following topics:

- Methods of Managing the Server Load Balancer
- Assigning an IP Address

Methods of Managing the Server Load Balancer

You can manage a Server Load Balancer using one of the following methods:

- *Web interface management* — Each Server Load Balancer has a set of internal Web pages that allow you to manage the Server Load Balancer using a Web browser. Using the Web interface is the preferred method of management.
- *Command line interface management* — The Server Load Balancer offers limited command line interface (CLI) commands to configure basic parameters, such as the management IP Address.
- *SNMP management* — You can manage a Server Load Balancer using any Network Manager running the Simple Network Management Protocol (SNMP), such as 3Com Network Supervisor software. SNMP management is limited and does not allow for full configuration functionality.

Assigning an IP Address

To manage a Server Load Balancer over the network, the Server Load Balancer must be initially configured with the following:

- An IP address and subnet mask
- A default route

The CLI provides a series of online instructions that you need to complete the setup process.

To assign an IP address to the Server Load Balancer, complete the following steps:

1. Connect your management station to the console port on the front the Server Load Balancer. See "Console Port Cable" on page 84.
2. On a Windows® PC, you may use the Hyperterminal program or other terminal emulator. The correct settings are:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: Hardware

3 Hit <Return>. At the `login:` prompt, enter **`admin`**.

The Server Load Balancer provides two levels of access, admin and monitor. The password field contains blank default login passwords. The two levels of access are:

- admin — the user can access and change all manageable parameters
- monitor — the user can view all manageable parameters, but cannot change any parameters

4 At the `password:` prompt, hit **`<Return>`**. The password field contains a blank default login password. The *Welcome to the SLB Setup* CLI appears.

***CAUTION**: The Server Load Balancer does not provide a way to recover a lost password. If you choose to assign a new password, it is suggested you keep note of it in a safe place. If you forget your password, you will be locked out of the unit. If you change the password during the CLI Server Load Balancer setup, this is the password you should use, and not the blank default login password. For Technical Support, see* Appendix C.

```
Welcome to the SLB Setup

Follow the on-screen instructions to complete the setup
process.

You may run setup later by typing “setup” at the SEC> prompt.
Setup will take you through the following steps:
SEC>

1.  Set unit ip address
2.  Set default route
3.  Set clock
4.  Set login password

You may use <CR> to skip a step.
Enter unit ip in this format: nnn.nnn.nnn.nnn/pp
where: nnn.nnn.nnn.nnn is IP address
 pp is address prefix
```

5 You are prompted to enter the following information:
   - **a** a unit IP address
   - **b** a default route
   - **c** the local time
   - **d** the local date
   - **e** the number of desired time zone (1-107 options)
   - **f** a new login password
   - **g** confirm new login password
6 Once you have completed the setup, exit the CLI.

You are now ready to access the Server Load Balancer Web interface. See "Accessing the Web Interface" on page 30.

4 Working With the Web Interface

This chapter describes how to access and use the web interface. It covers the following topics:

- Choosing a Browser
- Accessing the Web Interface
- Using the Web Interface
- Setting up SNMP Management
- Upgrading Operating Software

Choosing a Browser

To display the Web interface correctly, use one of the following Web browsers:

- Netscape Navigator® version 4.5 or above.
- Microsoft® Internet Explorer version 5.0 or above.

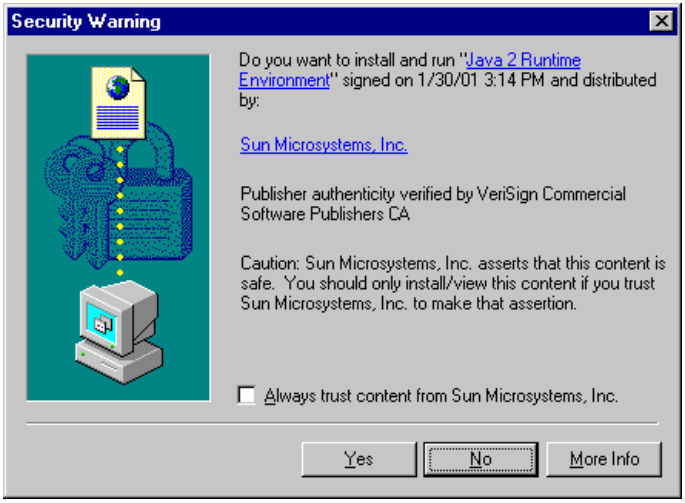
For the browser to operate the Web interface correctly, the Java Runtime Environment (JRE) V1.3.0_02 or higher must be installed on your management workstation.

A version of the JRE plug-in for Windows® is provided on the Server Load Balancer. If you do not already have the plug-in installed on your management station, you will be prompted to install it. See either "Installing the JRE for Microsoft Internet Explorer" or "Installing the JRE for Netscape Navigator".

Installing the JRE for Microsoft Internet Explorer

If you are using Microsoft Internet Explorer for your browser and do not have the Java Runtime Environment installed on your management station, the *Security Warning* window appears. Click *Yes* and follow the on-line instructions.

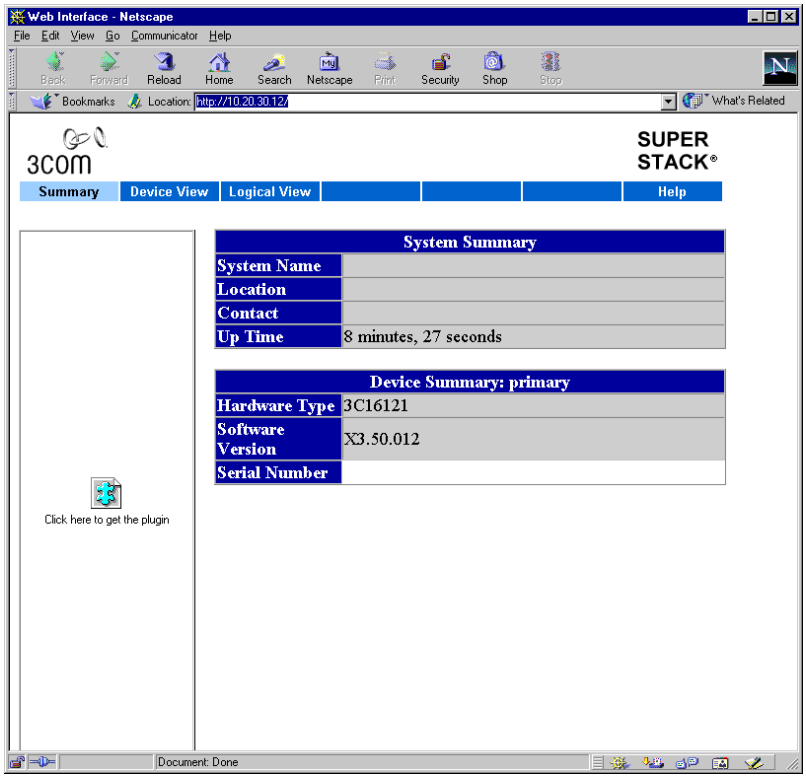
Figure 4 Security Warning Window



Installing the JRE for Netscape Navigator

If you are using Netscape Navigator for your browser and do not have the Java Runtime Environment installed on your management station, the *Web Interface* pages appears.

Figure 5 Web Interface - Netscape



To install the plug-in, complete the following steps:

1. Click on **`Click here to get the plug-in`**.
2. The *Plug-in Not Loaded* window appears. Click **`Get the plug-in`**. The *Plug-in Install for Netscape* page appears.
3. Click **`Download Plug-in`**. The *Save As* window appears.
4. Save the file to your Desktop.
5. From your desktop, double-click on **`jre1_3_0.exe`**.

   The Java Runtime Environment is now installed.

Accessing the Web Interface

To access the Web interface *over the network*, complete the following steps:

1. Ensure that your network is correctly set up for management using the Web interface and open your Web browser.
2. In the Location field of the browser, enter the URL of the Server Load Balancer. This must be in the format:

   `http://`*`nnn.nnn.nnn.nnn`*`/`

   where ***`nnn.nnn.nnn.nnn`*** is the IP address you assigned in "Assigning an IP Address" on page 24.

   When the browser has located the Server Load Balancer, the *Enter Network Password* window appears.
3. Enter **`admin`** in the *User Name* field.

   The Server Load Balancer provides two levels of access, admin and monitor. The password field contains a blank default login password. The two levels of access are:

   - admin — the user can access and change all manageable parameters
   - monitor — the user can view all manageable parameters, but cannot change any parameters
4. The password field contains a blank default login password. Hit <Return>.

CAUTION: *The Server Load Balancer does not provide a way to recover a lost password. If you choose to assign a new password, it is suggested you keep note of it in a safe place. If you forget your password, you will be locked out of the unit. If you change the password during the CLI Server Load Balancer setup, this is the password you should use, and not the blank default login password. For Technical Support, see* Appendix C.

The main Web interface is displayed. See "Using the Web Interface" on page 31.

Exiting the Web interface

You can exit the Web interface at any time; to do this, close your Web browser. For security reasons, you should always close your Web browser after a management session.

Using the Web Interface

The Web interface is made up of three areas:

- **The Banner**

  This is always displayed at the top of the browser window. It displays the name of the current Server Load Balancer, and contains several external links that allow you to access information outside of the Web interface.

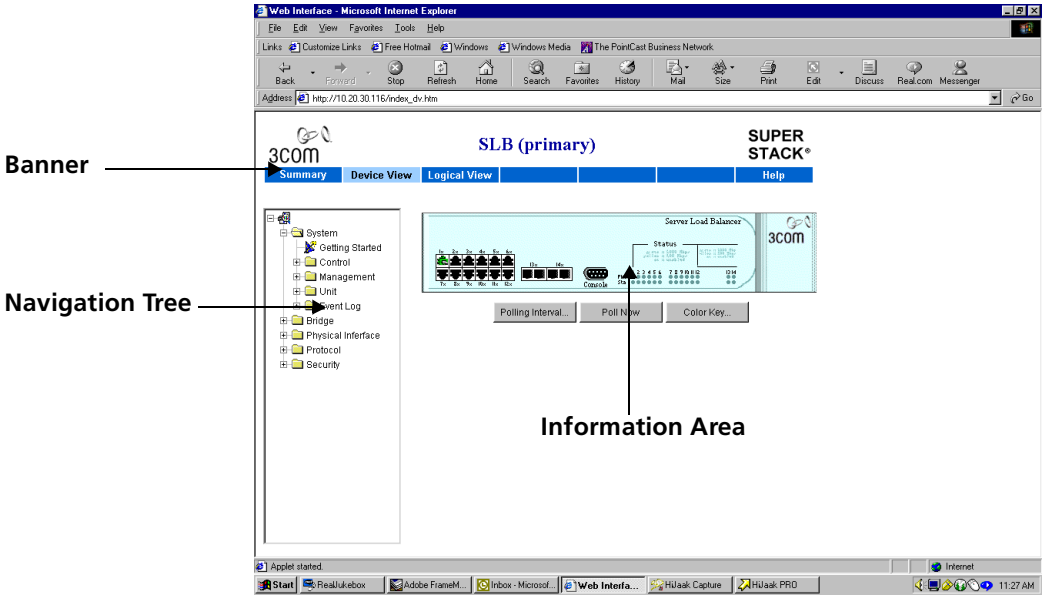
- **The Navigation Tree**

  This is always displayed down the left side of the browser window. It contains management folders that display dialog boxes in the information area.

- **The Information Area**

  This is always displayed in the center of the browser window. It contains the various dialog boxes that allow you to manage the Server Load Balancer.

Figure 6 Parts of the main Web interface

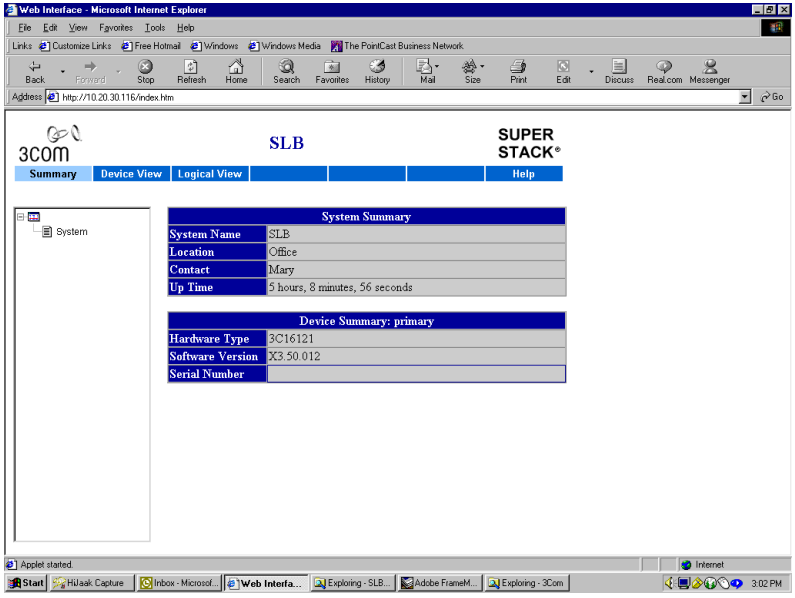


Summary View

The Summary View displays the latest information for the Server Load Balancer.

The Summary View only displays information for the Server Load Balancer. You cannot perform any operations from this view. You must use the Device View and the Logical View to perform operations.

Figure 7 Summary View



The summary information is displayed in a two tables:

- **System Summary**

  The first table is entitled System Summary and displays the System Name, Location, Contact and Up Time.

- **Device Summary**

  The second table is entitled Device Summary and displays the hardware type, software version, and serial number for the Server Load Balancer.

Device View

The Device View contains a mimic of the Server Load Balancer. The device mimic is an interactive representation of the Server Load Balancer. It is periodically updated to reflect changes, particularly changes made to the status of its ports. This view is used to configure fundamental system and port operating parameters. To configure server load balancing, cache redirection and other features, use the Logical View.

While the Device View allows you to configure using the graphical user interface, there are some features that can only be configured from the Navigation Tree.

You can setup the Server Load Balancer by two methods; through the Navigation Tree or by clicking on the following device mimic "hotspots":

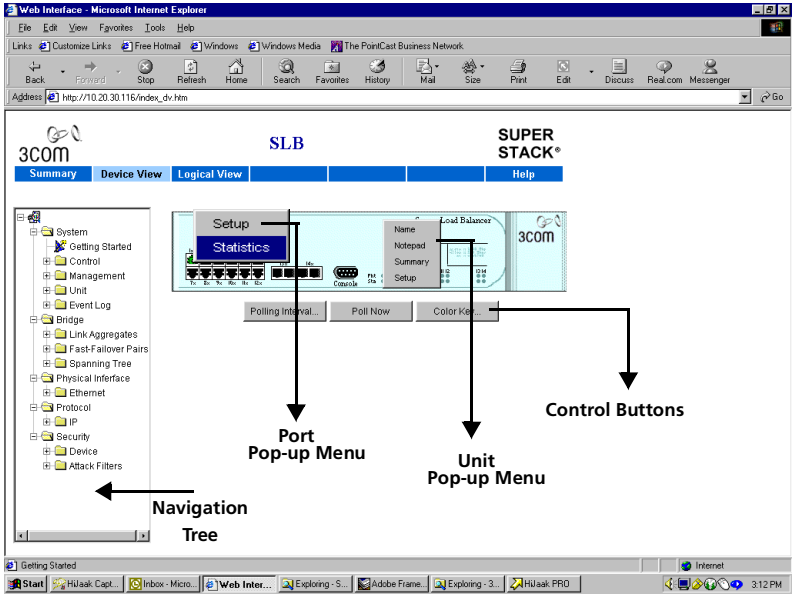
- **Port Hotspots**

  Each port on the mimic, including the console port, is a "hotspot". Click a port to open a pop-up menu that contains operations which you can launch for that particular port.

- **Unit Hotspot**

  The non-port area of the mimic is a "hotspot". Click anywhere on this area to open a pop-up menu that contains operations which you can launch for the Server Load Balancer as a whole.

Figure 8 Device View



Control Buttons

Beneath the device mimic are three control buttons that you can use to control the mimic and its appearance and to provide help information:

- *Polling Interval* — Click to set the rate at which the device mimic is refreshed.
- *Poll Now* — Click to refresh the mimic now.
- *Color Key* — Click for an explanation of the symbols and colors on the mimic's ports. Table 8 describes the colors and their actions.

Table 8 Color Key Codes

Color	Action
Green	Enabled, connected
Black	Enabled, disconnected
Gray (with connection)	Disabled, connected
Gray (without connection)	Disabled, disconnected

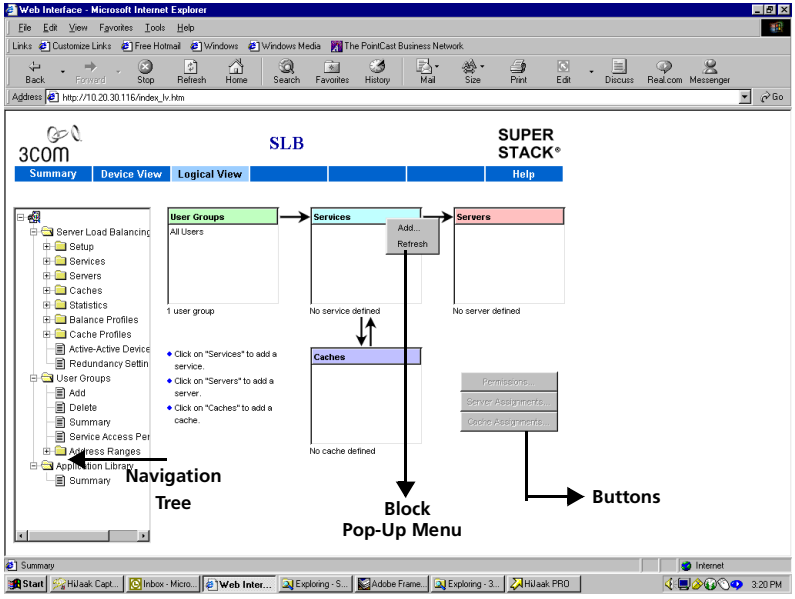
Logical View

The Logical View presents a graphical view of the Server Load Balancer configuration. This view is used to configure and monitor server load balancing, cache redirection and other high level device features. There are four blocks, each representing an area of configuration. Once configured, the entities will be listed in each block, and the approximate flow of data requests is indicated by the arrows.

You can configure the Server Load Balancer by two methods; through the Navigation Tree or by clicking on the top half of the block. Each colored portion of the block has a "hotspot". Click on a the block to open a pop-up menu that contains operations you can use to configure the Server Load Balancer.

While the Logical View allows you to configure using the graphical user interface, there are some features that can only be configured from the Navigation Tree.

Figure 9 Logical View



In addition to the blocks, there are three buttons that can be used to assign permissions, and server and cache assignments. Table 9 describes the buttons and their actions.

Table 9 Buttons and their actions

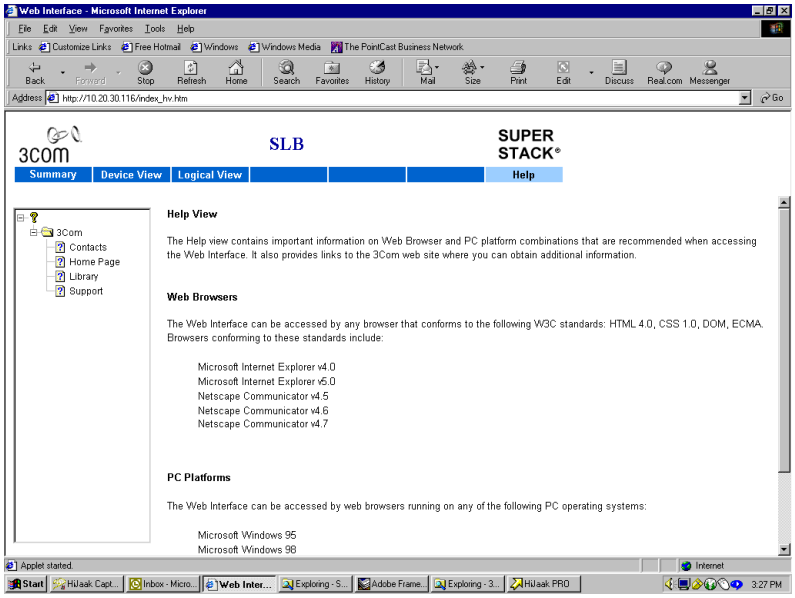
Button	Action
Permissions	Displays a matrix of user groups versus virtual services displaying access rights of deny or allow.
Server Assignments	Displays a matrix of virtual services versus physical servers. This display shows which servers are used for each virtual service and the operational status of the mappings.
Cache Assignments	Displays a matrix of cache servers. This display shows which cache server are used for each virtual service and the operational status of the mappings.

Help View

The Help view contains important information on Web Browser and PC platform combinations that are recommended when accessing the Web interface. The Help view also supplies minimal online user documentation.

If your management workstation has access to the World Wide Web, clicking these links displays information from the 3Com Web site in a second browser window.

Figure 10 Help View



Setting up SNMP Management

You can manage a Server Load Balancer using any Network Manager running the Simple Network Management Protocol (SNMP), such as 3Com Network Supervisor software.

Specifying Community Strings

You can specify SNMP community strings for the users defined on the Server Load Balancer.

To specify the community strings, complete the following steps:

1. Click *Device View* on the Toolbar.
2. Select *System* > *Management* > *Community Strings* in the Navigation Tree. The *Community Strings* window is displayed.
3. The *Get Access Community String* field is defaulted to *public*.
4. Select *Set Access Enabled* check box. This enables the access to the Server Load Balancer. The *Set Access Community Strin*g is defaulted to *private*.
5. Click *OK*.

Modifying a Trap Address

You can modify a trap address and its community string. The Server Load Balancer supports the following traps:

- Cold Start
- Authentication Failure
- Link Up/Down
- Spanning Tree newRoot
- Spanning Tree topologyChange
- RMON Event

To modify a trap address, complete the following steps:

1. Click *Device View* on the Toolbar.
2. Select *System* > *Management* > *Trap Address* in the Navigation Tree. The *Modify Trap Address* page appears. This page lists the ID, IP Address and the Community String.
3. Click on **2**. The line becomes highlighted.
4. Click *Modify*. The *Trap Address* window appears.
5. The *Trap Community String* field is defaulted to *public*.
6. Enter **1.1.1.1** in the *Trap IP Address* field. The IP address you enter should be the destination for this trap.
7. Click *OK* and close out of the *Modify Trap Address* page. You have now modified the trap community string and the trap IP address.

Upgrading Operating Software

You can upgrade the management software using the *Software Upgrade* window.

CAUTION: *It is suggested that when performing a software upgrade, you disable any security filters you have enabled. See* "Modifying Security Filters" *on* page 72***.***

To upgrade the software, complete the following steps:

1. Click *Device View* on the Toolbar.
2. Select *System* > *Control* > *Software Upgrade* in the Navigation Tree.
3. The *Software Upgrade* window is displayed.
4. Copy the software upgrade file into an appropriate directory on a TFTP server.
5. Enter the name of the software field in the *File name* field. The filename format is:

   `slbv350a.bin`

CAUTION*: You must use the* `slbv350a.bin` *format, otherwise the upgrade fails.*

6. Enter the IP address of the TFTP server in the *TFTP Server IP Address* field.
7. Click *OK*.

   During the upgrade, the Power/Self Test LED flashes green. The upgrade procedure takes about 5 minutes. When the upgrade is complete, the Server Load Balancer is reset.

CAUTION*: During the upgrade, do not power-down or reset the Server Load Balancer.*

5 CONFIGURING NON-REDUNDANT SERVER LOAD BALANCING

In this chapter, a typical non-redundant server load balancing scenario is presented, with instructions for configuring the Server Load Balancer.

The information presented in this chapter is for example purposes only and actual addresses will vary.

The following is a list of steps for the scenario presented for configuring non-redundant server load balancing. These steps explained in detail in this chapter are:

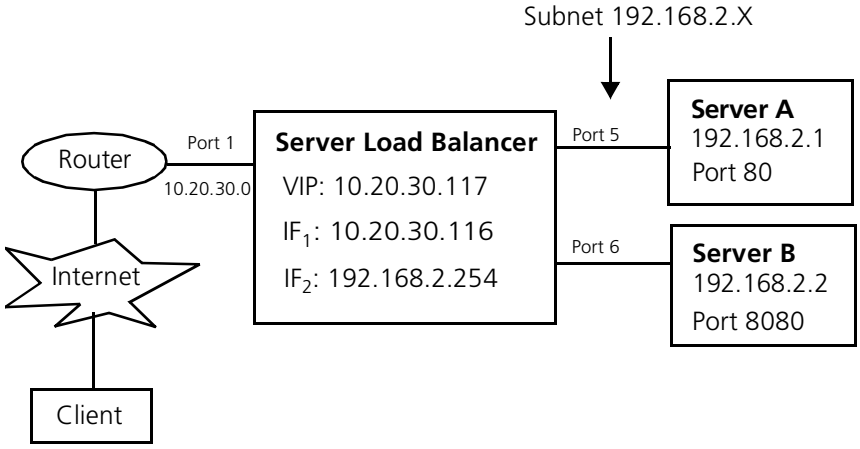
- Server Load Balancing Configuration Example
- Configuring for Non-redundant Server Load Balancing

Before you complete the steps explained in this chapter, you must have completed the assigning IP address setup described in Chapter 3 Setting Up for Management.

Server Load Balancing Configuration Example

Figure 11 displays a network configuration of two primary servers, Server A and Server B. The servers have been set up to host a Web site to the public. Server A is assumed to be a powerful machine that has approximately double the performance of Server B.

Figure 11 Server Load Balancing Configuration Example

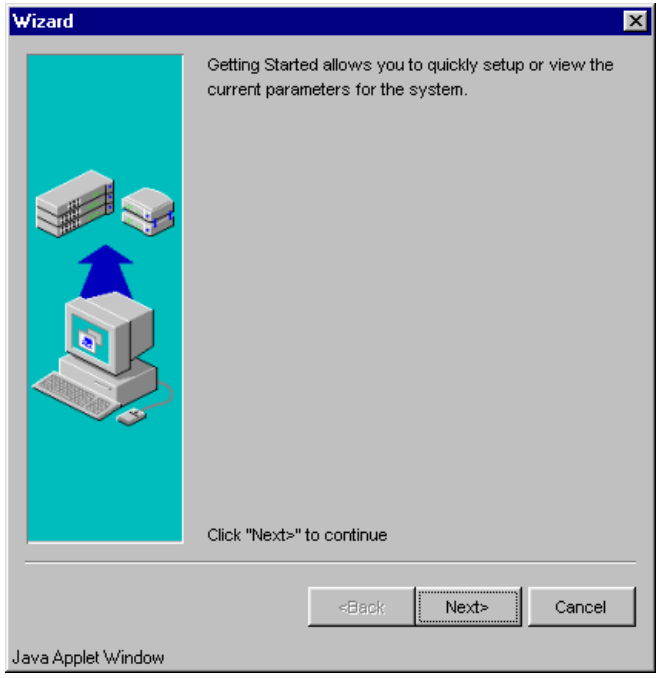


Configuring for Non-redundant Server Load Balancing

You must complete the steps in the *Getting Started* wizard to configure the Server Load Balancer for non-redundant server load balancing.

To setup up a non-redundant configuration, complete the following steps:

1. Click *Device View* on the Toolbar.
2. Select *System* > *Getting Started* in the Navigation Tree. The first Getting Started page is displayed. Click *Next*.



3 Enter a descriptive name, such as **`Non-redundant SLB`**, in the *Name* field.

4 Enter the name of the person to contact about the Server Load Balancer, such as **`Chris`**, in the *Contact* field.

5 Enter the physical location of the Server Load Balancer, such as **`Lab`**, in the *Location* field.

6 Click *Next*. The *Getting Started - Configuration* page appears.

7 Select *Non-Redundant*.

8 Click *Next*. The *Getting Started - IP Settings* page appears.

The IP Address, Subnet Mask and Default Router fields are completed. This is the information you assigned to the Server Load Balancer during the CLI setup.

If you change these settings, you may lose IP connectivity to the Web interface upon completion of this wizard. If this occurs, you will need to reconnect to the Server Load Balancer using the new IP address.

9 Click *Next*. The *Getting Started - Network Address Translation* page appears.

If you are using private IP subnets for your server or cache subnets and want the servers or caches to be able to initiate connections to the outside, check **`NAT Enabled for Server and Cache Subnets`**. If NAT is enabled, packets initiated by the servers and the caches need to be given an IP address on the primary IP subnet. This address is the alias address.

10 Click *Next*. The *Getting Started - Password* page appears.

CAUTION: *The Server Load Balancer does not provide a way to recover a lost password. If you choose to assign a new password, it is suggested you keep note of it in a safe place. If you forget your password, you will be locked out of the unit. If you change the password during the CLI Server Load Balancer setup, this is the password you should use, and not the blank default login password. For Technical Support information, see Appendix C.*

11 Click *Finish*. The parameters you have entered are ready to be applied.

You are now ready to configure the load balancing services. See Chapter 8 Configuring for Load Balancing.

6 CONFIGURING REDUNDANT SERVER LOAD BALANCING

In this chapter, a typical redundant server load balancing scenario is presented, with instructions for configuring the Server Load Balancer.

The information presented in this chapter is for example purposes only and actual addresses will vary.

The following is a list of steps for the scenario presented for configuring redundant server load balancing. These steps explained in detail in this chapter are:

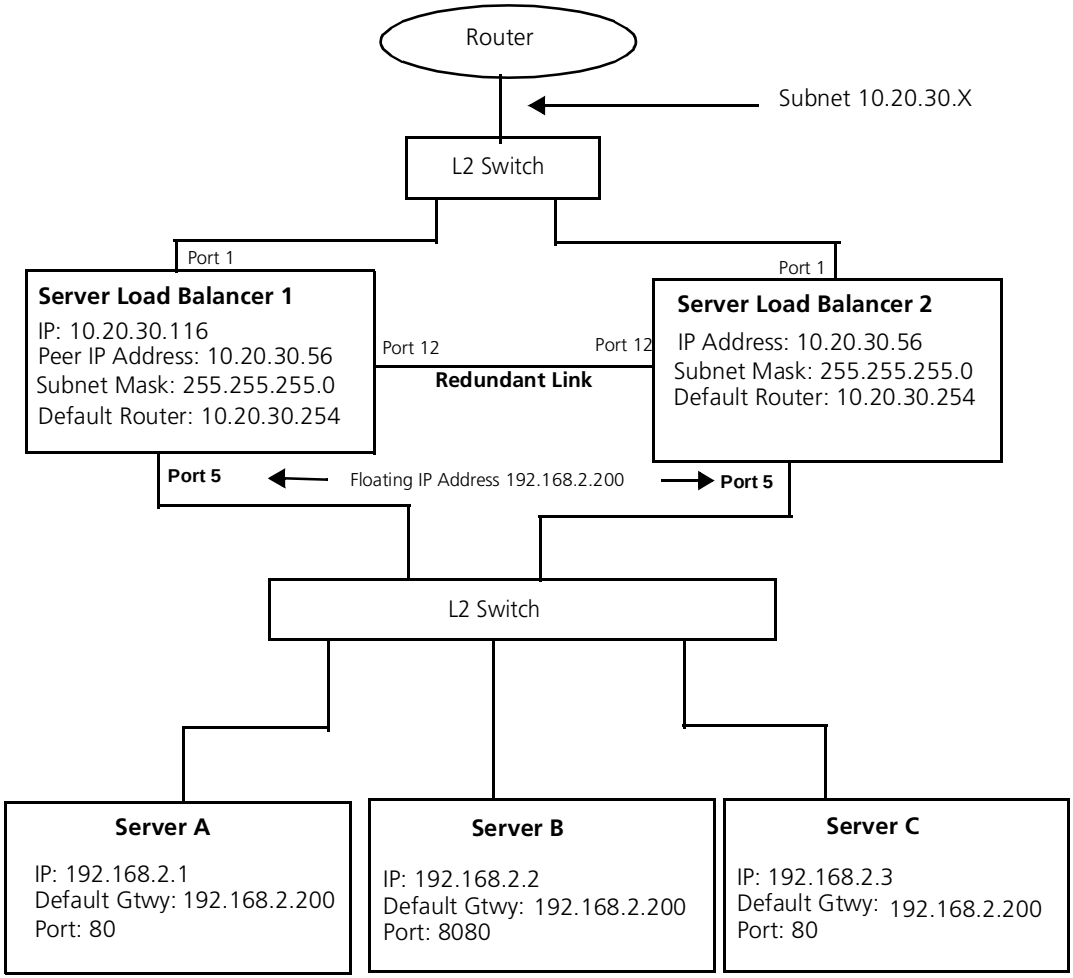
- Configuring for Active-Passive Redundancy
- Configuring for Active-Active Redundancy
- Active-Active Device Allocation
- Setting Redundancy Settings

Before you complete the steps explained in this chapter, you must have completed the preliminary setup described in Chapter 3 Setting Up for Management.

Redundant Server Load Balancing Configuration Example

Figure 12 shows how two Server Load Balancers and three servers form a redundant Web service. Server Load Balancer 1 is the Primary server load balancer which actively handles client requests sent to the VIP. Server Load Balancer 2 automatically recognizes the settings on Server Load Balancer 1 and is configured for the same service.

Figure 12 Redundant Server Load Balancing Configuration Example

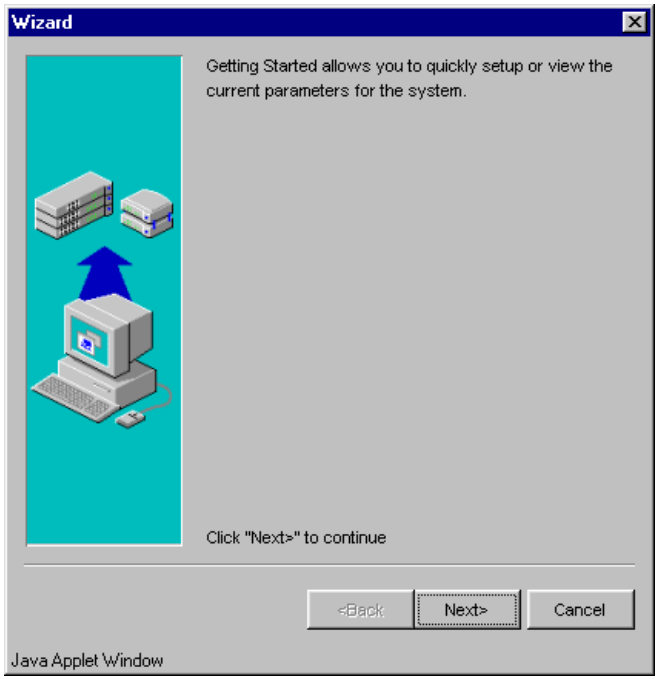


Configuring for Active-Passive Redundancy

You must complete the *Getting Started* wizard to configure the Server Load Balancer for active-passive redundancy.

To setup up a for active-passive redundancy configuration, complete the following steps:

1. Click *Device View* on the Toolbar.
2. Select *System* > *Getting Started* in the Navigation Tree. The first Getting Started page is displayed. Click *Next*.



3. Enter a descriptive name, such as **`Active-Passive`**, in the *Name* field.
4. Enter the name of the person to contact about the Server Load Balancer, such as **`Bob`**, in the *Contact* field.
5. Enter the physical location of the Server Load Balancer, such as **`Office`**, in the *Location* field. Click *Next*.
6. Select *Redundant.* The *Getting Started - Select Device B* page displays.

7 Select the serial number of Device B. In this case, this is the second Server Load Balancer.

If the device you wish to use as Device B does not appear in the list, check that the cable linking Device B to Device A is connected properly.

8 Click *Next.* The *Getting Started - IP Settings* page appears.

If you change these settings, you may lose IP connectivity to the Web interface upon completion of this wizard. If this occurs, you will need to reconnect to the Server Load Balancer using the new IP address

The IP Address, Subnet Mask and Default Router fields are completed. These is the information you assigned to the Server Load Balancer during the CLI setup.

9 Enter **`10.20.30.56`** in the *Device B IP Address* field.

This is the IP address assigned to the second Server Load Balancer.

10 Click *Next*. The *Getting Started - Network Address Translation* page appears.

If you are using private IP subnets for your server or cache subnets and want the servers or caches to be able to initiate connections to the outside, check **`NAT Enabled for Server and Cache Subnets`**. If NAT is enabled, packets initiated by the servers and the caches need to be given an IP address on the primary IP subnet. This address is the alias address.

11 Click *Next.* The *Getting Started - Password* page appears.

CAUTION: *The Server Load Balancer does not provide a way to recover a lost password. If you choose to assign a new password, it is suggested you keep note of it in a safe place. If you forget your password, you will be locked out of the unit. If you change the password during the CLI Server Load Balancer setup, this is the password you should use, and not the blank default login password. For Technical Support information, see Appendix C.*

12 Click *Next.* The *Getting Started - Advanced* page appears

13 Click *Continue with Advanced Settings* and click *Next.*

14 Select *Active-Passive* and click *Next*. The *Getting Started - Summary* page appears.

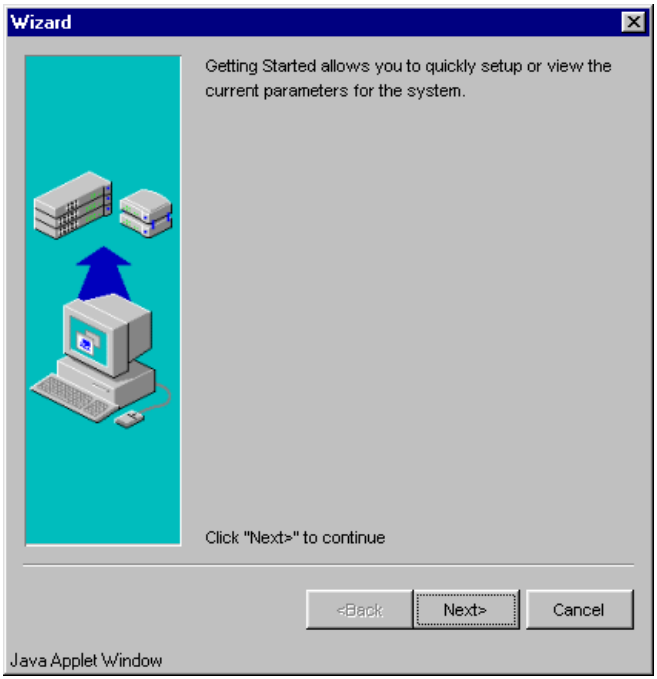
15 Click *Finish*. Your parameters you have entered are ready to be applied.

Configuring for Active-Active Redundancy

You must complete the *Getting Started* wizard to configure the Server Load Balancer for active-active redundancy.

To setup up an active-active redundancy configuration, complete the following steps:

1. Click *Device View* on the Toolbar.
2. Select *System* > *Getting Started* in the Navigation Tree. The first Getting Started page is displayed. Click *Next*.



3. Enter a descriptive name, such as **`Active-Active`**, in the *Name* field.
4. Enter the name of the person to contact about the Server Load Balancer, such as **`Dave`**, in the *Contact* field.
5. Enter the physical location of the Server Load Balancer, such as **`Lab`**, in the *Location* field. Click *Next*.
6. Select *Redundant* and click *Next*. The *Getting Started - Peer* page displays. Click *Next*.

7 Select the serial number of the peer device. In this case, the peer device is the second Server Load Balancer.

8 Click *Next.* The *Getting Started - IP Settings* page appears.

If you change these settings, you may lose IP connectivity to the Web interface upon completion of this wizard. If this occurs, you will need to reconnect to the Server Load Balancer using the new IP address.

9 The IP Address, Subnet Mask and Default Router fields are completed. These is the information you assigned to the Server Load Balancer during the CLI setup.

10 Enter **`10.20.30.56`** in the *Device B IP Address* field.

This is the IP address assigned to the second Server Load Balancer.

11 Click *Next*. The *Getting Started - Network Address Translation* page appears.

If you are using private IP subnets for your server or cache subnets and want the servers or caches to be able to initiate connections to the outside, check **`NAT Enabled for Server and Cache Subnets`**. If NAT is enabled, packets initiated by the servers and the caches need to be given an IP address on the primary IP subnet. This address is the alias address.

12 Click *Next.* The *Getting Started - Password* page appears.

CAUTION: *The Server Load Balancer does not provide a way to recover a lost password. If you choose to assign a new password, it is suggested you keep note of it in a safe place. If you forget your password, you will be locked out of the unit. If you change the password during the CLI Server Load Balancer setup, this is the password you should use, and not the blank default login password. For Technical Support information, see Appendix C.*

13 Click *Next.* The *Getting Started - Advanced* page appears

14 Click *Continue with Advanced Settings* and click *Next.*

15 Select *Active-Active* and click *Next*. The *Getting Started - Summary* page appears.

16 Click *Finish*. The parameters you have entered are ready to be applied.

You are now ready to configure the load balancing services. See Chapter 8 Configuring for Load Balancing.

Active-Active Device Allocation

Active-Active device allocation can only be performed when the Server Load Balancer has been configured to be redundant and active-active. The Active-Active device allocation page allows you to allocate which services are currently active on the two redundant Server Load Balancers. You can allocate FTP to one Server Load Balancer and HTTP to the other. The two Server Load Balancers each provide only the allocated services, until a failover occurs.

To setup up a active-active device allocation, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. Select *Server Load Balancing* > *Active-Active Device*. *The Active-Active Device Allocation* page is displayed.
3. Choose the virtual host(s) you wish to change the position of.
4. Click on the host and then click the appropriate arrow.

You are now ready to configure the load balancing services. See Chapter 8 Configuring for Load Balancing.

Setting Redundancy Settings

Whether you are configured for non-redundant or redundant server load balancing, if there are multiple Server Load Balancers, the Virtual Router Identifier (VRID) for each device must be unique or the service may not come up and one of the other Server Load Balancers declares itself the primary device.

To enter a unique number for the VRID, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. Select *Server Load Balancing* > *Redundancy Setting* in the Navigation Tree. The *Redundancy Settings* page is displayed.
3. Enter **25** in the *Virtual router ID A* field.
4. Enter **26** in the *Virtual router ID B* field.
5. Click *OK*.

7 CONFIGURING CACHE REDIRECTION

In this chapter, a typical application redirection scenario is presented, with directions for configuring the Server Load Balancer.

The information presented in this chapter is for example purposes only and actual addresses will vary.

The following list provides a checklist of the configuration steps for the scenario presented for configuring cache redirection on the Server Load Balancer. These steps are explained in detail in this chapter:

- Defining a Cache Subnet
- Non-redundant Configuration
- Redundant Configuration
- Adding a Cache
- Assigning Caches to Services
- Creating a Cache Profile (Optional)

Cache Redirection Configuration Example

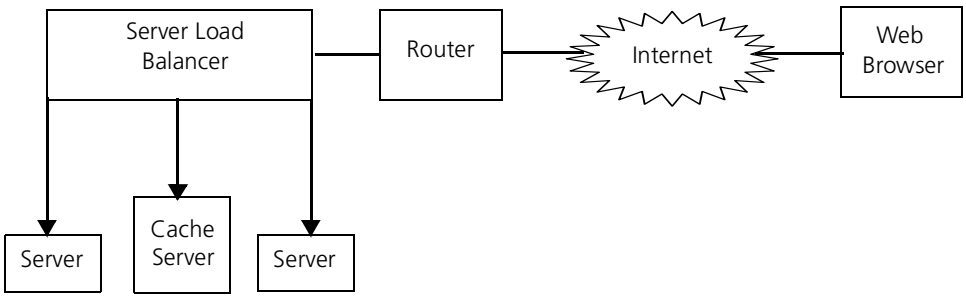
Figure 13 illustrates a sample network configuration for cache redirection. This example displays how cache redirection works.

A request is entered into the browser, for example, http://www.3Com.com. The browser then sends the request to the Server Load Balancer.

The Server Load Balancer looks at the protocol and determines that it is the HTTP protocol and forwards the request to the cache server.

Upon receipt of the request, the cache server determines whether it has a local copy of the requested page. If not, the cache server sends its own request to www.3Com.com. When www.3Com.com responds to the cache server, the cache server forwards the response to the client, and if permitted, makes a local copy.

Figure 13 Cache Redirection Configuration Example



Defining a Cache Subnet

Before you can add a cache, you need to have defined at least one cache subnet.

The cache subnet cannot be in the same subnet as the server.

Non-redundant Configuration

The following steps describe how to create a cache subnet if you are configured for non-redundant server load balancing.

To create a cache subnet, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. From the Navigation tree, select *System* > *Setup* > *Cache Subnets*.
3. Click *Add*. The first wizard page appears.
4. Click *Next*. The *Cache Subnet - Configure Address* page appears.
5. Enter **`192.168.3.200`** in the IP Address field.
6. Enter **`255.255.255.0`** in the Subnet Mask field.
7. Click *Next.* The *Cache Subnet - Floating Address* page appears.
8. Complete the entry in the Floating Address field. This is the floating default gateway IP address. For example, **`192.168.3.150`**.

Do not forget to change the default gateway on your caches to this IP address.

9. Click *Next*. The *Cache Subnet* page appears.
10. Click *Finish*. Your cache subnet has been added.

Redundant Configuration

The following steps describe how to create a cache subnet if you are configured for redundant server load balancing.

The cache subnet cannot be in the same subnet as the server.

To create a cache subnet, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. From the Navigation tree, select *System* > *Setup* > *Cache Subnets*.
3. Click *Add*. The first wizard page appears.
4. Click *Next*. The *Cache Subnet - Configure Address* page appears.
5. Enter **`192.168.3.200`** in the *Device A IP Address* field.
6. Enter **`192.168.3.100`** in the *Device B IP Address* field.
7. Enter **`255.255.255.0`** in the Subnet Mask field.
8. Click *Next.* The *Cache Subnet - Device A Floating Address* page appears.
9. Complete the entry in the *Device A Floating Address* field. This is the floating default gateway IP address. For example, **`192.168.3.150`**.

Do not forget to change the default gateway on your caches to this IP address.

10. Click *Next*.
11. Click *Finish*. Your cache subnet has been added.

Adding a Cache

This is where the cache service is defined, along with several attributes of the service.

1. Click *Logical View* on the Toolbar.
2. Point to the *Cache* window border and left-click the mouse button.
3. In the pop-up list, click *Add*. The *Configure Cache* page appears.

If you have not defined a cache subnet, you will be prompted with a Warning message asking if you wish to define the cache subnet now. See "Defining a Cache Subnet" on page 58.

4. Complete the entry in the IP Address field. For example, **`192.168.3.1`**.
5. Enter **Cache1** in the Name field.
6. Select the cache type and click *Add*. There are two available cache types:
   - Transparent
   - Proxy
7. Click *Done*.

Assigning Caches to Services

The *Assign Caches to Services* page is where the caches are assigned to cache redirection.

The Cache Assignments button is highlighted only if an HTTP service has been created.

1. Click *Cache Assignments*. The *Assign Caches to Services* page appears.
2. Click on the cell to assign a cache service.
3. Click on the cell next to **Cache1**. The *Assign cache to service* pop-up menu appears.
4. Click *Assign cache to service*. The cell for Server A is assigned.
5. Repeat the above steps for each of the caches you have created.

Showing Status and Deleting the Cache

To view the status of the cache assignments, complete the following steps:

1. Click *Cache Assignments*. The *Assign Caches to Services* page appears
2. Click the cell for *Cache1*. A pop-up menu with the option to *Show status* or *Delete* appears.
   a. If you wish to view the status of the server, click *Show status*. The *Mapping Status* dialog appears. This dialog box tells you the status of the service running on the assigned cache server.
   b. If you wish to delete the cache from the service, click *Delete*. You are prompted with a message asking you if you are sure you want to delete the cache from the service.
3. Repeat the above steps for each of the servers you have assigned.

Creating a Cache Profile (Optional)

You can create a unique cache profile that specifies a specific algorithm and assign a health check to monitor the status of the servers. You can set the health parameters and assign the number of retries, seconds (period) and timeout seconds.

A default cache profile set to Round-robin exists and will work for most applications.

To create a cache profile, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. From the Navigation tree, select *Server Load Balancing > Cache Profiles.*
3. Click *Add*. The first wizard page appears.
4. Click *Next*. The *Cache Profile Configuration - General Information* page appears.
5. Enter a descriptive name, such as **`Cache2`**, in the *Name* field.

6 Choose a algorithm. The default algorithm is *Round-robin*. Table 10 describes the available algorithms.

Table 10 Supported Algorithms and Description

Supported Algorithms	Description
Destination	The Destination IP address of the client's packets is hashed and used as an index to an array of active servers bound to the service. This is appropriate for redirection of sessions between a smaller set of clients and a larger set of servers, for example, local users of the extraNet, or the World-Wide Web
Round Robin	Each new connection is assigned to the next server in the list. This distributes connections evenly between the servers.
Weighted Round Robin	Similar to Round Robin, except that *N* consecutive new connections are assigned to a server before selecting the next server in the list, where N is the weight assigned to the server. Servers with higher performance or capacity should be assigned higher weight. The weight assigned to the server is assigned using the *Assign caches to services (Advanced)...* window. A weight field is provided.
Least Connections	Each new connection is assigned to the server having the fewest number of open connections. If several servers have the same low number of open connections, then the new connection is sent to the server that was least recently sent a new connection
Weighted Least Connections	Similar to Least Connections, except that *N* consecutive new connections are assigned to a server before next selecting the server with the least number of open connections, where N is the weight assigned to the server

7 Leave Sticky Mode field set to *Off*.

8 The default health check is *Ping*, click *Next.* Other available health checks are:

- *Ping* — Server Load Balancer periodically pings each server using ICMP Echo. The number of retries are configurable. If successive ping attempts fail, the server is marked as down and is removed from the pool of available servers.

- *TCP Port* — Server Load Balancer periodically attempts to establish a connection with each server using the same protocol (TCP or UDP) and port number as the server load balancing service uses. If any connection attempt fails, the server is marked as down and is removed from the pool of available servers for the service.
- *None* — No health checking is performed. All Servers are assumed to be operational.

9 The *Cache Profile Configuration - Health Checks* page appears. This page supplies default settings, which can be modified for your network, for the following fields:

- *Period*

  This sets the number of seconds that elapse between health checks.

- *Retries field*

  This sets the number of retries a health check is attempted.

- *Timeout*

  This sets the number of seconds the Server Load Balancer waits for a reply before the health check is timed out.

10 Click *Next*.

11 Click *Finish*.Your cache profile has been created.

8 CONFIGURING FOR LOAD BALANCING

In this chapter the instructions for configuring User Groups, Services and Servers on the Server Load Balancer are explained. It also explains how to configure for cache redireciton.

The information presented in this chapter is for example purposes only. The information you enter in the fields is specific to your Server Load Balancer.

The following is a list of steps for the scenario presented for configuring server load balancing and cache redirection on the Server Load Balancer. These steps explained in detail in this chapter are:

- Defining a Server Subnet
- Changing Lan Port Roles
- Adding a Server
- Adding a Service
- Assigning Servers to Service
- Adding a User Group
- Creating a Balance Profile (Optional)
- Modifying Security Filters (Attack Mitigation)

Before you complete the steps explained in this chapter, you must have completed the preliminary setup described in Chapter 3 Setting Up for Management and in either Chapter 5 Configuring Non-redundant Server Load Balancing or Chapter 6 Configuring Redundant Server Load Balancing.

Defining a Server Subnet

Before you can add a server, you need to have defined at least one server subnet. The default gateway of each server must be set to the floating default gateway address of the Server Load Balancer.

To define a server subnet, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. From the Navigation tree, select *Server Load Balancing* > *Setup* -> *Server Subnets*.
3. Click *Add*. The first wizard page appears.
4. Click *Next*. The *Server Subnet - Define Subnet* page appears.
5. Enter **`192.168.2.254`** in the IP Address field.

   If configuring for a redundant configuration, you need to enter the IP addresses of both Device A and Device B.
6. Enter **`255.255.255.0`** in the Subnet Mask field.
7. Click *Next.* The *Server Subnet - Device A Floating Address* page appears
8. Complete the entry in the *Floating Address* field. For example, **`192.168.2.200`**.

Do not forget to change the default gateway on your servers to this IP address

9. Click *Finish*. Your server subnet has been added.

Changing Lan Port Roles

When configuring server load balancing, the physical ports that carry client or server traffic can be specified. Each port is assigned to one of the following:

- *User Access* — Defines a port through which clients can access the Server Load Balancer.
- *Cache Access* — Defines a port to which a cache device is connected.
- *Server Access* — Defines a port to which servers are connected, either directly or through a network switch.
- *Management Access* — Defines the port used for management access to the Server Load Balancer. If no Management Access port is specified, you can manage the Server Load Balancer through any user access port.
- *Redundant Link* — Defines the port connected as a redundant link to another Server Load Balancer. Only one redundant link port is allowed.

To change Lan port roles, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. Select *Server Load Balancing* > *Setup* > *Lan Port Roles* in the Navigation Tree. The *Lan Port Roles* page appears.
3. Click a port to open a pop-up menu that contains operations which you can set for that particular port.
4. Choose the access you want. For example, if you wish to assign port 1 from the current access to Server Access, complete the following:
   a. Click on the port for *1.* A pop-up menu appears with a list of port roles.
   b. Click *Server Access*. The *Saving Data* window appears and the port changes color.
   c. Click *Close*.

Adding a Server

The servers must first be defined before they can be bound to a particular service. The server is given an arbitrary name (this does not have to be its DNS name) and is identified by its IP address.

To define a server, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. Point to the *Server* window border and left-click the mouse button.
3. In the pop-up list, click *Add*. The first *Configure Server* page appears.

If you have not defined a server subnet, you will be prompted with a Warning message asking if you wish to define the server subnet now. If you click Yes, follow the online instructions. For information on how to configure a Server Subnet, see "Defining a Server Subnet" on page 62.

4. Enter **`192.168.2.1`** in the *IP Address* field and click *Add*
5. Enter **`Server A`** in the *Name* field.
6. Repeat steps 4 and 5 for each server you are adding.
7. Click *Done*.

   The servers are now known to the Server Load Balancer, but are not associated with a service.

Adding a Service

This is where the load balancing service is defined, along with several attributes of the service. Remember that the service is associated with an IP address (the VIP) and a protocol/port combination (the application).

To define a service, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. Point to the *Services* window border and left-click the mouse button.
3. In the pop-up list, click *Add*. The first wizard page appears.
4. Click *Next*. The *Add Service - Application Definition* page appears
5. Enter a descriptive name, such as **`Web`**, in the *Name* field.
6. Click *Choose application from application library*. You are presented with a list of applications, grouped by application type.
7. Highlight *HTTP* and click the *Next*.
8. Click *Define new virtual IP address* and enter **`10.20.30.117`** in the Virtual IP Address field. The VIP address has to be in the same subnet as the Server Load Balancer.
9. Enter a descriptive name, such as **`HTTP Service`**, in the *Name* field.
10. Click *Continue with Advanced Settings*.
11. From the Balance Profile drop-down list box, select *Profile1*.

If you have not created a balance profile, the drop-down list box only provides a default. See "Creating a Balance Profile (Optional)" on page 69.

12. Skip the *Add Service - Port Override* page. Click *Next*. The port override allows you to change the destination port that (TCP or UDP) requests will come into.
13. Click *Finish*. This completes the set up of the service.

    The service name you added, Web, now appears in the lower portion of the block. Click on a the block to open a pop-up menu that contains operations you can use to Add, Refresh, Delete, Modify, or Show Status of the service.

Assigning Servers to Service

The *Assign Servers to Services* page is where the servers are assigned to the server load balancing service.

To assign a server to a service, complete the following steps:

1. Click *Server Assignments*. The *Assign servers to services* page appears.
2. Click on the cell next to *Server A*. The *Assign server to service* pop-up menu appears.
3. Click *Assign server to service*. The cell for Server A is assigned.
4. Repeat the above steps for each of the servers you have created.

Showing Status and Deleting the Server

To show the status of a server assignments or to delete one, complete the following steps:

1. Click *Server Assignments*. The *Assign servers to services* page appears
2. Click the cell for Server A. A pop-up menu with the option to *Show status* or *Delete* appears.
   a. If you wish to view the status of the server, click *Show status*. The *Mapping Status* dialog appears. This dialog box tells you the status of the service running on the assigned server.
   b. If you wish to unassign the server, click *Delete*. You are prompted with a message asking you if you are sure you want to delete the server from the service.
3. Repeat the above steps for each of the servers you want unassigned.

Assigning Server to Services (Advanced)

In addition to performing Network Address Translation, the Server Load Balancer is capable of translating the TCP or UDP port on which the service is operating. The virtual service can be configured for a well known port, while the servers respond to an alternate port. For example, a Web service is set up on the standard TCP port 80 and translated to 8080. When a request is received from a client on port 80, the Server Load Balancer changes the port to 8080 before forwarding the packet on to one of the available servers. When the server reply is received by the Server Load Balancer, it changes the port number back to 80, then forwards the packet on to the client.

To change the port, complete the following steps:

1. Click *Server Assignments*.
2. Click on the cell next to *Server A*. A pop-up menu appears.
3. Click *Assign server to service (Advanced)...*. The *Assign Server to Service* window appears.
4. Enter **8080** in the Server port field.
5. Click *OK*.

Adding a User Group

You can define a user group and control that group's access to the load balanced services. For each request to a service, the Server Load Balancer determines which user group the client IP address is part of. It then allows or denies access to the service based on the permissions that were set for this user group.

The Server Load Balancer has a default user group that is defined as 0.0.0.0 to 255.255.255.255. This user group includes every possible IP address.

To add a user group, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. Point to the *User Group* window border and left-click the mouse button.
3. In the pop-up list, click *Add*. The *Add User Group* window appears.
4. Enter a descriptive name, such as **`Engineering`**, in the *Name* field.

It is recommended to keep the user group name to a maximum of 20 characters.

5. Repeat Step 4 for every user group you wish to add and click *Add*.
6. When you have finished entering your user groups, click *Done*.

Adding IP Address Ranges to User Groups

Adding IP address ranges defines those IP addresses that make up your user group. The Server Load Balancer recognizes any address within these ranges to be part of the user group.

If a request comes, the Server Load Balancer determines that the client is part of the Engineering user group and checks the permissions set for Engineering for the service requested.

To add IP address ranges to your user group, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. Point to the *User Group* window border and left-click the mouse button.
3. In the pop-up list, click *Add address range...*
4. From the *User Group* drop-down list box, select *Engineering*.
5. Enter **`192.168.1.100`** in the *First IP Address* field.
6. Enter **`192.168.1.150`** in the *Last IP Address* field and click *Done*.

Accessing Permissions

You can change user access on specific servers using the *Permissions* button. You are able to allow or deny access for assigned user groups.

To assign permissions, complete the following steps:

1. Click *Permissions*.
2. Click on the cell next to *Server A*. Depending on the access already set, you are prompted with either *Deny Access* or *Allow Access*.
3. Click the access you wish to set. The icon changes.
4. Click *OK*.

Creating a Balance Profile (Optional)

You can create a unique balance profile that specifies a specific algorithm and assign a health check to monitor the status of the servers. You can set the health parameters and assign the number of retries, seconds (period) and timeout seconds.

A default balance profile set to Round-robin exists and will work for most applications.

To create a balance profile, complete the following steps:

1. Click *Logical View* on the Toolbar.
2. From the Navigation tree, select *Server Load Balancing* > *Balance Profiles.*
3. Click *Add*. The first wizard page appears.
4. Click *Next*. The *Balance Profile Configuration - General Information* page appears.
5. Enter a descriptive name, such as **`Profile1`**, in the *Name* field.

6 Choose a balancing algorithm. The default balance profile is *Round-robin*. Table 11 describes the available algorithms.

Table 11 Supported Algorithms and Descriptions

Supported Algorithms	Description
Round Robin	Each new connection is assigned to the next server in the list. This distributes connections evenly between the servers.
Weighted Round Robin	Similar to Round Robin, except that *N* consecutive new connections are assigned to a server before selecting the next server in the list, where N is the weight assigned to the server. Servers with higher performance or capacity should be assigned higher weight. The weight assigned to the server is assigned using the *Assign server to service (Advanced)...* window. A weight field is provided.
Least Connections	Each new connection is assigned to the server having the fewest number of open connections. If several servers have the same low number of open connections, then the new connection is sent to the server that was least recently sent a new connection
Weighted Least Connections	Similar to Least Connections, except that *N* consecutive new connections are assigned to a server before next selecting the server with the least number of open connections, where N is the weight assigned to the server
Quickest Last Response	When a new connection is established between a client and server, the Server Load Balancer monitors the client's first request for data. When the server responds to the initial request, the Server Load Balancer notes the time delay between the request and the response and stores that value as the server's response time. Each new connection is sent to the server having the fastest response time. Since server response time changes dynamically, a decay algorithm is applied periodically to all response times to prevent a server from being locked out after one long response delay
Quickest Average Response	Similar to Quickest Last Response, except the response time is averaged over approximately the last eight measurements for the server. A decay algorithm is also applied to the average response times

7 Leave Sticky Mode field set to *Off*.

8 The default health check is *Ping*, click *Next.* Other available health checks are:

- *Ping* — Server Load Balancer periodically pings each server using ICMP Echo. The number of retries are configurable. If successive ping attempts fail, the server is marked as down and is removed from the pool of available servers.
- *TCP Port* — Server Load Balancer periodically attempts to establish a connection with each server using the same protocol (TCP or UDP) and port number as the server load balancing service uses. If any connection attempt fails, the server is marked as down and is removed from the pool of available servers for the service.
- *HTTP URI* — You can enter a URI that the Server Load Balancer periodically requests from each server. A server response is considered successful if the return code of response is within the range of 200-299. If any attempts fail, the server is marked as down and is removed from the pool of available servers for the service. This performs a more thorough check of the status of the Web servers.
- *None* — No health checking is performed. All Servers are assumed to be operational.

9 The *Balance Profile Configuration - Health Checks* page appears. This page supplies default settings, which can be modified for your network, for the following fields:

- *Period*

  This sets the number of seconds that elapse between health checks.

- *Retries field*

  This sets the number of retries in a health check period.

- *Timeout*

  This sets the number of seconds the Server Load Balancer waits for a health check reply from a server.

10 Click *Next*.

11 Click *Finish*. Your balance profile has been created.

Modifying Security Filters (Attack Mitigation)

The Server Load Balancer provides Attack Mitigation features that help to prevent Denial of Service and Distributed Denial of Service attacks.

When enabled, the attack mitigation features cause the Server Load Balancer to recognize and filter out security attacks. Table 12 describes the available filters and their descriptions.

Table 12 Filters and Descriptions

Filter	Description
Smurf Filter	Filter ICMP packets sent to broadcast or multicast addresses and unsolicited ICMP ECHO replies
FTP Restricted Port Filter	Filter out a range of FTP data port requests.
IP Source Route Filter	Filter packets which contain the IP source route option.
LAND Attack	Filter packets which have matching destination and source IP addresses.
Fraggle Attack Filter	Filter UDP ECHO requests sent to a broadcast or multicast address and unsolicited UDP packets from the UDP ECHO port.
FTP Bounce Filter	Filter FTP traffic when the port command issued contains an address that differs from the requesting host.
IP Options Filter	Filter packets that contain any IP options (for example, Record Route and Time Stamp) in the packet header. You can filter packets which have packet headers containing only the Strict Source Route and Loose Source Route IP options using the IP Source Route filter

Modifying Security Filters

To modify the security filters, complete the following steps:

1. Click *Device View* on the Toolbar.
2. Select *Security* > *Attack Filters*.
3. Click *Modify*. The *Modify Attack Filters* page appears.
4. Select the attack filters you wish to enable and click *OK*.

Modifying User Access

To modify the access of either the admin or monitor user, complete the following steps:

1. Click *Device View* on the Toolbar.
2. Select *Security* > *User*.
3. You can modify the user access for either the admin or monitor.

Modifying Admin Access

a To modify the admin access, click *Modify Admin*. The *Modify Password* page appears.

b Enter a new password and confirm.

Modifying Monitor Access

a To modify the monitor access, click *Modify Monitor*. The *Modify Password* page appears.

b Enter a new password and confirm.

CAUTION: *The Server Load Balancer does not provide a way to recover a lost password. If you choose to assign a new password, it is suggested you keep note of it in a safe place. If you forget your password, you will be locked out of the unit. If you change the password during the CLI Server Load Balancer setup, this is the password you should use, and not the blank default login password. For Technical Support, see Appendix C.*

A SAFETY INFORMATION

You must read the following safety information before carrying out any installation or removal of components, or any maintenance procedures on the Server Load Balancer or the Server Load Balancer Plus.

WARNING: *Warnings contain directions that you must follow for your personal safety. Follow all directions carefully.*
You must read the following safety information carefully before you install or remove the unit.

AVERTISSEMENT: *Les avertissements présentent des consignes que vous devez respecter pour garantir votre sécurité personnelle. Vous devez respecter attentivement toutes les consignes.*
Nous vous demandons de lire attentivement les consignes suivantes de sécurité avant d'installer ou de retirer l'appareil.

WARNHINWEIS*: Warnhinweise enthalten Anweisungen, die Sie zu Ihrer eigenen Sicherheit befolgen müssen. Alle Anweisungen sind sorgfältig zu befolgen.*
Sie müssen die folgenden Sicherheitsinformationen' sorgfältig durchlesen, bevor Sie das Gerät installieren oder ausbauen.

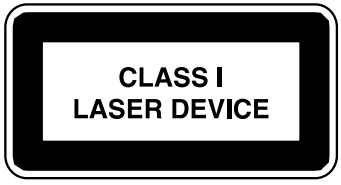
Important Safety Information

- Installation and removal of the unit must be carried out by qualified personnel only.
- If installing the Server Load Balancer in a stack with SuperStack 3 units that are narrower than the Server Load Balancer, the Server Load Balancer unit must be installed below the narrower units.
- Connect the unit to an earthed power supply to ensure compliance with safety standards.
- Power Cord Set:
  This must be approved for the country where it is used:

U.S.A. and Canada	■ The cord set must be UL-approved and CSA certified. ■ The minimum specification for the flexible cord is: No. 18 AWG Type SV or SJ 3-conductor ■ The cord set must have a rated current capacity of at least 10A. ■ The attachment plug must be an earth-grounding type with a NEMA 5-15P (15A, 125V) or NEMA 6-15P (15A, 250V) configuration.
United Kingdom only	■ The supply plug must comply with BS1363 (3-pin 13 amp) and be fitted with a 5A fuse which complies with BS1362. ■ The mains cord must be <HAR> or <BASEC> marked and be of type H03VVF3GO.75 (minimum).
Europe only:	■ The supply plug must comply with CEE 7/7 (“SCHUKO”). ■ The mains cord must be <HAR> or <BASEC> marked and be of type H03VVF3GO.75 (minimum).
Denmark	■ The supply plug must comply with section 107-2-D1, standard DK2-1a or DK2-5a.
Switzerland	■ The supply plug must comply with SEV/ASE 1011.

- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN60320/IEC320 appliance inlet.
- The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.

- This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.
- France and Peru only:
  This unit cannot be powered from IT† supplies. If your supplies are of IT type, this unit must be powered by 230V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labelled Neutral, connected directly to earth (ground).
  †Impédance à la terre.
- The switch should only be used in a rack if it is mounted on runners, a shelf, or a tray to support the weight. The rack mount kits alone are not sufficient to support the weight of the switch. The rack mount kits must not be used to suspend the switch from under a table or desk, or attach it to a wall.
- If you are connecting the Server Load Balancer to a Type 3 Power Module, read the Safety Information section in the Type 3 Power Module User Guide.
- WARNING: Fiber Optic ports - Optical Safety



- Never look at the transmit laser while it is powered-up. Never look directly at the fiber TX port and fiber cable ends when they are powered-up.
- Use of controls or adjustments of performance or procedures other than those specified herein may result in hazardous laser emissions.

L'information de Sécurité Importante

- L'installation et la dépose de ce groupe doivent être confiés à un personnel qualifié.
- Si vous entassez l'unité Switch avec les unités SuperStack 3 Hub, l'unité Server Load Balancer doit être installée en dessous des unités Hub plus étroites.
- Brancher l'unité à une source de courant mise à la terre pour assurer la conformité aux normes de sécurité.
- Cordon électrique:
  Il doit être agréé ans le pays d'utilisation:

Etats-Unis et Canada	■ Le cordon doit avoir reçu l'homologation des UL et un certificat de la CSA ■ Le cordon souple doit respecter, à titre minimum, les spécifications suivantes : ■ calibre 18 AWG ■ type SV ou SJ ■ à 3 conducteurs ■ Le cordon doit être en mesure d'acheminer un courant nominal d'au moins 10 A ■ La prise femelle de branchement doit être du type à mise à la terre (mise à la masse) et respecter la configuration NEMA 5-15P (15 A, 125 V) ou NEMA 6-15P (15 A, 250 V)
Danemark	■ La prise mâle d'alimentation doit respecter la section 107-2 D1 de la norme DK2 1a ou DK2 5a
Europe	■ La prise secteur doit être conforme aux normes CEE 7/7 ("SCHKO") ■ LE cordon secteur doit porter la mention <HAR> ou <BASEC> et doit être de type HO3VVF3GO.75 (minimum).
Suisse	■ La prise mâle d'alimentation doit respecter la norme SEV/ASE 1011

- Le coupleur d'appareil (le connecteur du groupe et non pas la prise murale) doit respecter une configuration qui permet un branchement sur une entrée d'appareil EN60320/CEI 320.
- La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.

- L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme CEI 950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.
- France et Pérou uniquement:
  Ce groupe ne peut pas être alimenté par un dispositif à impédance à la terre. Si vos alimentations sont du type impédance à la terre, ce groupe doit être alimenté par une tension de 230 V (2 P+T) par le biais d'un transformateur d'isolement à rapport 1:1, avec un point secondaire de connexion portant l'appellation Neutre et avec raccordement direct à la terre (masse).
- Le commutateur doit être utilisé en rack uniquement s'il est monté sur des rails à glissières, une étagère ou un plateau pour supporter son poids. Les kits de montage en rack ne suffisent pas à eux seuls pour supporter le poids du commutateur.
- Si vous connectez le commutateur Server Load Balancer à un moduled'alimentation de Type 3, consultez les informations de sécurité qui se trouvent dans le guide del'utilisateur du module d'alimentation de type 3.

AVERTISSEMENT: Ports pour fibres optiques – sécurité sur le plan optique

- Ne regardez jamais le laser tant qu'il est sous tension. Ne regardez jamais directement le port TX (Transmission) à fibres optiques et les embouts de câbles à fibres optiques tant qu'ils sont sous tension.
- L'utilisation de contrôles, de réglages de performances ou de procédures autres que ceux qui sont spécifiés au sein du présent document risquent d'entraîner l'exposition à des rayonnements laser dangereux.

Wichtige Sicherheitsinformationen

- Die Installation und der Ausbau des Geräts darf nur durch Fachpersonal erfolgen.
- Wenn die Server Load Balancer Einheit in einer Stapel mit anderen SuperStack 3 Hub Einheiten eingebaut werden soll, muß die Server Load Balancer Einheit unter die schmaleren Hub Einheiten eingebaut werden.
- Das Gerät muß an eine geerdete Steckdose angeschlossen werden, die europäischen Sicherheitsnormen erfüllt.
- Der Anschlußkabelsatz muß mit den Bestimmungen des Landes übereinstimmen, in dem er verwendet werden soll.
- Der Gerätestecker (der Anschluß an das Gerät, nicht der Wandsteckdosenstecker) muß eine passende Konfiguration für einen Geräteeingang gemäß EN60320/IEC320 haben.
- Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.

Europe

  - Das Netzkabel muß vom Typ HO3VVF3GO.75 (Mindestanforderung) sein und die Aufschrift <HAR> oder <BASEC> tragen.
  - Der Netzstecker muß die Norm CEE 7/7 erfüllen ("SCHUKO").

- Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.
- Der Switch darf nur dann in einem Einschub montiert werden, wenn dieser zur Tragkraftverstärkung auf einer Laufschiene, in einem Regal oder einem Träger montiert ist. Der Einschubmontagesatz alleine reicht nicht aus, um das Gewicht des Switch zu tragen.
- Ist kein Erweiterungsmodul installiert, überprüfen Sie bitte den Sitz der Stanzplatte, indem Sie alle Schrauben mit einem geeigneten Werkzeug anziehen.
- Bevor Sie den Schalter Server Load Balancer an das Stromversorgungsmodul Typ 3 anschließen, lesen Sie bitte die Sicherheitshinweise in der Bedienungsanleitung für das Stromversorgungsmodul Typ 3.

***ACHTUNG**: Faseroptikanschlüsse – Optische Sicherheit*

- Niemals ein Übertragungslaser betrachten, während dieses eingeschaltet ist. Niemals direkt auf den Faser-TX-Anschluß und auf die Faserkabelenden schauen, während diese eingeschaltet sind.
- Die Verwendung von Steuerelementen oder die Anpassung von Leistungen und Verfahren in anderer als der hierin genannten Weise kann zu gefährlichen Laseremissionen führen.

B TECHNICAL SPECIFICATIONS AND PIN-OUTS

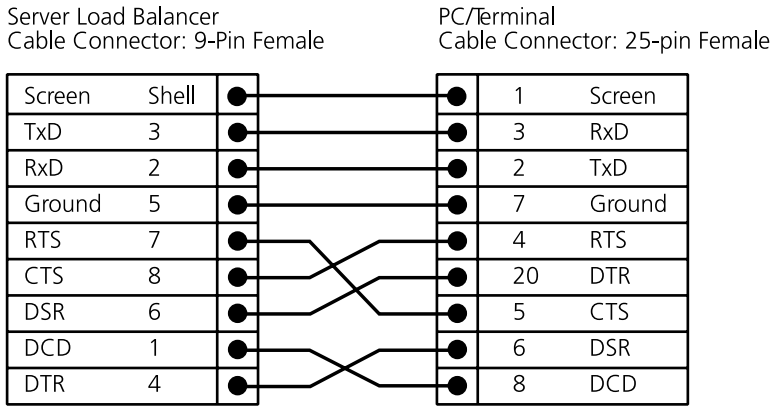
Server Load Balancer Specifications

The following table lists the technical specifications for the Server Load Balancer and the Server Load Balancer Plus:

Physical Dimensions	Height: 65.8 mm (2.59 in.) x Width: 440 mm (17.3 in.) x Depth: 368.4 mm (14.5 in.). Weight: 6.6 Kg (14.55 lbs)
Environmental Requirements	
Operating Temperature	0 ° to 40 °C (32 ° to 104 °F)
Storage Temperature	–40 ° to +70 °C (–8 ° to 158 °F)
Operating Humidity	10–95% relative humidity, non-condensing
Standards	EN60068 to 3Com schedule (Package testing: paras 2.1, 2.2, 2.30, and 2.32. Operational testing: paras 2.1, 2.2, 2.30 and 2.13).
Safety	
Agency Certifications	UL 1950, EN60950, CSA 22.2 No. 950, IEC 60950, IEC 825-1, EN 60825-1
EMC	
Emissions	CISPRR 22 Class A, EN55022 (1998) Class A, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class A, AS/NZS 3548 Class A, CNS 13438 Class A, EN61000-3-2
Immunity	EN 55024 (1998)
Heat Dissipation	250 watts maximum (850 BTU/hour maximum)
Power Supply	
AC Line Frequency	50/60 Hz
Input Voltage Options	100–240 VAC
Current Rating	3 A (amps) (maximum)

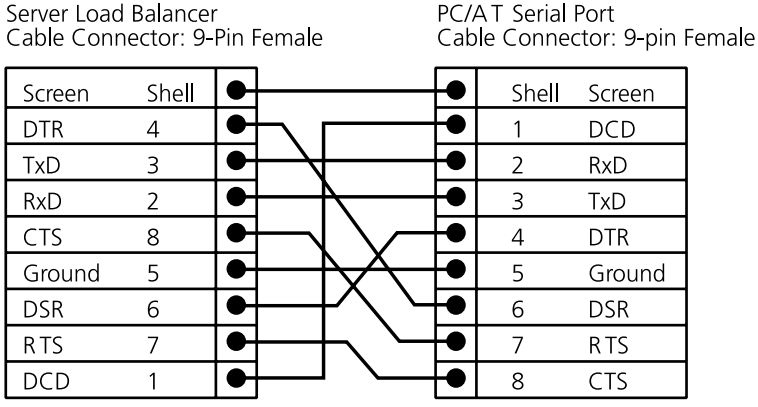
Console Port Cable

9-pin to RS232 25-pin



PC-AT Serial

9-pin to 9-pin



C TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the most recent information, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com Knowledgebase Web Services
- 3Com FTP site

World Wide Web Site

To access the latest networking information on the 3Com Corporation World Wide Web site, enter this URL into your Internet browser:

`http://www.3com.com/`

This service provides access to online support information such as technical documentation and software, as well as support options that range from technical education to maintenance and professional services.

3Com Knowledgebase Web Services

This interactive tool contains technical product information compiled by 3Com expert technical engineers around the globe. Located on the World Wide Web at **`http://knowledgebase.3com.com`**, this service gives all 3Com customers and partners complementary, round-the-clock access to technical information on most 3Com products.

3Com FTP Site

Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **`ftp.3com.com`**
- Username: **`anonymous`**
- Password: **`<your Internet e-mail address>`**

You do not need a user name and password with Web browser software such as Netscape Navigator and Internet Explorer.

Support from Your Network Supplier

If you require additional assistance, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, call the 3Com technical telephone support phone number at the location nearest you.

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Here is a list of worldwide technical telephone support numbers. These numbers are correct at the time of publication. Refer to the 3Com Web site for updated information.

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim			
Australia	1 800 678 515	P.R. of China	10800 61 00137 or
Hong Kong	800 933 486		021 6350 1590 or
India	+61 2 9937 5085 or		00800 0638 3266
	000800 6501111	Singapore	800 6161 463
Indonesia	001 800 61 009	S. Korea	00798 611 2230 or
Japan	03 5783 1270		02 3455 6455
Malaysia	1800 801 777	Taiwan, R.O.C.	00798 611 2230
New Zealand	0800 446 398	Thailand	0080 611 261
Pakistan	+61 2 9937 5083		001 800 611 2000
Philippines	1235 61 266 2602		
Europe, Middle East and Africa			
From anywhere in these regions, call:	+44 (0)1442 435529 phone +44 (0)1442 436722 fax		

Country	Telephone Number	Country	Telephone Number
Europe and South Africa From the following countries, you may use the toll-free numbers:			
Austria	0800 297468	Luxembourg	0800 3625
Belgium	0800 71429	Netherlands	0800 0227788
Denmark	800 17309	Norway	800 11376
Finland	0800 113153	Poland	00800 3111206
France	0800 917959	Portugal	0800 831416
Germany	0800 1821502	South Africa	0800 995014
Hungary	06800 12813	Spain	900 983125
Ireland	1800 553117	Sweden	020 795482
Israel	1800 9453794	Switzerland	0800 55 3072
Italy	800 8 79489	U.K.	0800 966197
Latin America			
Brazil	0800 13 3266	Puerto Rico	800 666 5065
Mexico	01 800 849CARE	Central and South America	AT&T +800 998 2112
North America	1 800 NET 3Com (1 800 638 3266)		
	Enterprise Customers: 1 800 876-3266		

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain an authorization number. Products sent to 3Com without authorization numbers will be returned to the sender unopened, at the sender's expense. To obtain an authorization number, call or fax:

Country	Telephone Number	Fax Number
Asia, Pacific Rim	+ 65 543 6500	+ 65 543 6348
Europe, South Africa, and Middle East	+44 (0)1442 435529	+ 44 (0)1442 436722
Central and South America	525 201 0075	
Argentina	0810 222 3266	
Bolivia	511 241 1691	
Brazil	0800 133266 or 55 11 5643 2700	
Caribbean	525 201 0004	
Chile	562 240 6200	
Colombia	525 201 0004	
Ecuador	525 201 0004	
Mexico	525 201 0004	
Paraguay	525 201 0004	
Peru	511 241 1691	
Uruguay	525 201 0004	
Venezuela	525 201 0004	
From the following countries, you may call the toll-free numbers; select option 2 and then option 2:		
Austria	0800 297468	
Belgium	0800 71429	
Denmark	800 17309	
Finland	0800 113153	
France	0800 917959	
Germany	0800 1821502	
Hungary	00800 12813	
Ireland	1800553117	
Israel	1800 9453794	
Italy	1678 79489	
Netherlands	0800 0227788	
Norway	800 11376	
Poland	00800 3111206	
Portugal	0800 831416	
South Africa	0800 995014	
Spain	900 983125	
Sweden	020 795482	
Switzerland	0800 55 3072	
U.K.	0800 966197	
U.S.A. and Canada	1 800 NET 3Com (1 800 638 3266) Enterprise Customers: 1 800 876 3266	1 408 326 7120 (not toll-free)

INDEX

3Com Corporation LIFETIME LIMITED WARRANTY

The 3Com Corporation Limited Warranty and the Other Services described in this document supersede any such information that may be contained within your product user documentation.

This warranty applies to customers located in the United States, Australia, Canada (except Quebec), Ireland, New Zealand, U.K., and other English language countries, and countries for which a translation into the local language is not provided.

SUPERSTACK® 3 SERVER LOAD BALANCER (3C16120)
SUPERSTACK® 3 SERVER LOAD BALANCER PLUS (3C16121)

HARDWARE:

3Com warrants to the end user ("Customer") that this hardware product will be substantially free from material defects in workmanship and materials, under normal use and service, for the following length of time from the date of purchase from 3Com or its authorized reseller:

Lifetime, for as long as the original Customer owns the product or for 5 years after product discontinuance, whichever occurs first (not transferable to a subsequent end user).

3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products or parts may be new or reconditioned. 3Com warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

SOFTWARE:

3Com warrants to Customer that each software program licensed from it, except as noted below, will perform in substantial conformance to its published program specifications, for a period of ninety (90) days from the date of purchase from 3Com or its authorized reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided under this warranty. 3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to refund the purchase price paid by Customer for any defective software product, or to replace any defective media with software which substantially conforms to applicable 3Com published program specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials.

3Com makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product or from use of the software product not in accordance with 3Com's published specifications or user manual.

THIS 3COM PRODUCT MAY INCLUDE OR BE BUNDLED WITH THIRD PARTY SOFTWARE. THE WARRANTY PROVISIONS OF THIS DOCUMENT DO NOT APPLY TO SUCH THIRD PARTY SOFTWARE. IF A SEPARATE END USER LICENSE AGREEMENT HAS BEEN PROVIDED FOR SUCH THIRD PARTY SOFTWARE, USE OF THAT SOFTWARE WILL BE GOVERNED BY THAT AGREEMENT. FOR ANY APPLICABLE WARRANTY, PLEASE REFER TO THE END USER LICENSE AGREEMENT GOVERNING THE USE OF THAT SOFTWARE.

SOFTWARE LICENSE AGREEMENT:

3Com grants you a nonexclusive, nontransferable (except as specified herein) license to use the accompanying software program(s) in executable form (the "Software") and accompanying documentation (the "Documentation"), subject to the terms and restrictions set forth in this Agreement. You are not permitted to lease, rent, distribute or sublicense (except as specified herein) the Software or Documentation or to use the Software or Documentation in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the Software (source code). Except as provided below, this Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights with respect to the Software or Documentation.

Subject to the restrictions set forth herein, the Software is licensed to be used on any workstation or any network server owned by or leased to you, for your internal use, provided that the Software is used only in connection with this 3Com product. You may reproduce and provide one (1) copy of the Software and Documentation for each such workstation or network server on which the Software is used as permitted hereunder. Otherwise, the Software and Documentation may be copied only as essential for backup or archive purposes in support of your use of the Software as permitted hereunder. Each copy of the Software and Documentation must contain 3Com's and its licensors' proprietary rights and copyright notices in the same form as on the original. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation delivered to you under this Agreement.

ASSIGNMENT; NO REVERSE ENGINEERING:

You may transfer the Software, Documentation and the licenses granted herein to another party in the same country in which you obtained the Software and Documentation if the other party agrees in writing to accept and be bound by the terms and conditions of this Agreement. If you transfer the Software and Documentation, you must at the same time either transfer all copies of the Software and Documentation to the party or you must destroy any copies not transferred. Except as set forth above, you may not assign or transfer your rights under this Agreement.

Modification, reverse engineering, reverse compiling, or disassembly of the Software is expressly prohibited. However, if you are a European Union ("EU") resident, information necessary to achieve interoperability of the Software with other programs within the meaning of the EU Directive on the Legal Protection of Computer Programs is available to you from 3Com upon written request.

EXPORT RESTRICTIONS:

The Software, including the Documentation and all related technical data (and any copies thereof) (collectively "Technical Data"), is subject to United States Export control laws and may be subject to export or import regulations in other countries. In addition, the Technical Data covered by this Agreement may contain data encryption code which is unlawful to export or transfer from the United States or country where you legally obtained it without an approved U.S. Department of Commerce export license and appropriate foreign export or import license, as required. You agree that you will not export or re-export the Technical Data (or any copies thereof) or any products utilizing the Technical Data in violation of any applicable laws or regulations of the United States or the country where you legally obtained it. You are responsible for obtaining any licenses to export, re-export or import the Technical Data. In addition to the above, the Product may not be used, exported or re-exported (i) into or to a national or resident of any country to which the U.S. has embargoed; or (ii) to any one on the U.S. Commerce Department's Table of Denial Orders or the U.S. Treasury Department's list of Specially Designated Nationals.

TRADE SECRETS:

You acknowledge and agree that the structure, sequence and organization of the Software are the valuable trade secrets of 3Com and its suppliers. You agree to hold such trade secrets in confidence. You further acknowledge and agree that ownership of, and title to, the Software and Documentation and all subsequent copies thereof regardless of the form or media are held by 3Com and its suppliers.

TERM AND TERMINATION:

The licenses granted hereunder are perpetual unless terminated earlier as specified below. You may terminate the licenses and this Agreement at any time by destroying the Software and Documentation together with all copies and merged portions in any form. The licenses and this Agreement will also terminate immediately if you fail to comply with any term or condition of this Agreement. Upon such termination you agree to destroy the Software and Documentation, together with all copies and merged portions in any form.

SEVERABILITY:

In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired and a valid, legal and enforceable provision of similar intent and economic impact shall be substituted therefor.

ENTIRE AGREEMENT:

This Agreement sets forth the entire understanding and agreement between you and 3Com and supersedes all prior agreements, whether written or oral, with respect to the Software and Documentation, and may be amended only in a writing signed by both parties.

Should you have any questions concerning this Agreement or if you desire to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write:

3Com Corporation
Customer Support Information
5400 Bayfront Plaza
P.O. Box 58145
Santa Clara, CA 95052-8145

OBTAINING WARRANTY SERVICE:

Customer must contact a 3Com Corporate Service Center or an Authorized 3Com Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from 3Com or its authorized reseller may be required. A User Service Order (USO), Return Material Authorization (RMA) or Service Repair Order (SRO) number will be issued. This number must be marked on the outside of the package. The product must be packaged appropriately for safe shipment and sent prepaid. It is recommended that returned products be insured or sent by a method that provides for tracking of the package. Responsibility for loss or damage does not transfer to 3Com until the returned item is received by 3Com. 3Com will make commercially reasonable efforts to ship the repaired or replaced item to Customer, at 3Com's expense, not later than thirty (30) days after 3Com receives the defective product. 3Com will retain risk of loss or damage until the item is delivered to Customer.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

WARRANTIES EXCLUSIVE:

IF THIS 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THIS WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT AND QUIETENJOYMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF THIS PRODUCT.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, POWER CUTS OR OUTAGES, OTHER HAZARDS, OR ACTS OF GOD.

LIMITATION OF LIABILITY:

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS LICENSORS AND SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

DISCLAIMER:

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for death or personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW:

This Limited Warranty shall be governed by the laws of the State of California, U.S.A., and by the laws of the United States, excluding their conflicts of laws principles. The United Nations Convention on Contracts for the International Sale of Goods is hereby excluded in its entirety from application to this Limited Warranty.

3Com Corporation, 5400 Bayfront Plaza, P.O. Box 58145, Santa Clara, CA 95052-8145 (408) 326-5000

March 13, 2001

OTHER SERVICES

3COM RESERVES THE RIGHT TO MODIFY OR CANCEL THESE SERVICES AT ANY TIME, WITHOUT ADVANCE NOTICE. THESE SERVICES ARE NOT AVAILABLE WHERE PROHIBITED OR RESTRICTED BY LAW. THESE SERVICES APPLY TO THE ORIGINAL CUSTOMER ONLY.

Free Advanced Hardware Replacement for 5 Years from date of purchase. Replacement will be shipped within 5 business days of 3Com receiving the request and is subject to conditions [1].

Free Software Updates will be provided for as long as the original customer owns the product until the product is discontinued by 3Com. All software and firmware upgrades for this product can be downloaded through the 3Com Software Library at http://support.3com.com.

REGISTER ONLINE FOR FREE SERVICE UPGRADE:

REGISTER ONLINE at http://support.3com.com within 30 days of purchase and qualify for the following discretionary services:

Free "Next Business Day Delivery" Advance Hardware Replacement for the first 12 months, and after that, the level offered will be five business days for years 2, 3, 4 and 5 of the life of the product, subject to conditions [1]. To check that your product and location qualify for the next business day advance hardware replacement see http://support.3com.com/registration/docs/hw_repl.html.

FREE telephone technical support for 12 months with real-time call handling during normal business hours [2].
Please refer to the Technical Support appendix in the User Guide for telephone numbers.

Find out more when you register online at: http://support.3com.com

[1] Shipment of a Replacement Prior to 3Com Receiving the Defective Product only if Customer provides a purchase order number, credit card number, or other method of payment acceptable to 3Com, to be used if 3Com needs to charge Customer for the replacement, as explained below. 3Com will make commercially reasonable efforts to ship the replacement product not later than five (5) business days after receiving the request for a replacement, or deliver the replacement by the next business day if the customer has registered, but may be delayed due to product availability or export or import procedures. Request for next business day replacements must be received by 3:00pm local time to be able to meet shipping deadline. The shipment of a replacement product prior to 3Com receiving the defective product is subject to local legal requirements and may not be available in all locations. When such a replacement is provided and Customer fails to return the original product to 3Com within fifteen (15) days after receipt of the replacement, 3Com will charge Customer for the replacement, at list price. Customer must ensure defective product is packaged appropriately for safe shipment and sent prepaid to 3Com. This replacement prior to 3Com receiving the defective product is different from the fee-based Advance Hardware Replacement Service, which is available as a contracted service offering.

[2] Telephone Technical Support will be provided for 12 months from the date of purchase, on a commercially reasonable efforts basis. Normal business hours may vary by geography, contact your local 3Com office for more information.

OTHER USEFUL WEB SITE SERVICES PROVIDED BY 3COM INCLUDE:

- A list of additional documents, release notes and frequently asked questions at: www.3com.com
- Full electronic product support information at: http://knowledgebase.3com.com
- Information about additional maintenance service options at: http:/www.3com.com/products/services/maint_services.html

REGULATORY NOTICES

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference to radio communications, in which case the user will be required to correct the interference at their own expense.

INFORMATION TO THE USER

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.

CSA STATEMENT

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

CE STATEMENT (EUROPE)

This product complies with the European Low Voltage Directive 73/23/EEC and EMC Directive 89/336/EEC as amended by European Directive 93/68/EEC.

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

VCCI STATEMENT

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI STATEMENT

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。